T-TeleSec MailPass
Trust Center Service für sichere E-Mail

Benutzerhandbuch

Version: 0.5
Stand: 09.08.2002

T-Systems
MV-Systems, T-TeleSec
Untere Industriestraße 20
57238 Netphen

Deutsche
Telekom

INHALTSVERZEICHNIS

1 EINLEITUNG 4

2 PKI-GRUNDLAGEN 5

2.1 Schlüssel und Zertifikate 5

2.2 Das Trust Center und der Domain-Betreiber 5

2.3 Smartcards und Software-PSEs 6

2.4 Single Key / Dual Key 6

3 AUFGABEN DES BENUTZERS 7

4 KOMPONENTEN 8

4.1 Voraussetzungen 8

4.2 Benutzer-Web-Schnittstelle 9

4.3 Eingeschränkte Benutzer-Web-Schnittstelle 10

4.4 Mail-Request-Schnittstelle 11

4.5 LDAP-Schnittstelle 11

4.6 OCSP-Schnittstelle 11

4.7 Sub-Registrator 11

4.8 Zentrale Sperr-Hotline 12

4.9 MailPass-Verantwortlicher 12

5 PROZESSE 13

5.1 Beantragen eines Zertifikats 13
5.1.1 Zentrale Registrierung beim Einsatz von Smartcards 14
5.1.2 Zentrale Registrierung beim Einsatz von Software-PSEs 15
5.1.3 Dezentrale Registrierung über die Web-Schnittstelle beim Einsatz von Smartcards 16
5.1.4 Dezentrale Registrierung über die Web-Schnittstelle beim Einsatz von Software-PSEs 23
5.1.5 Dezentrale Registrierung über die Mail-Request-Schnittstelle 30

5.2 Sperren eines Zertifikats 31
5.2.1 Sperren eines Zertifikats über die (eingeschränkte) Benutzer-Web-Schnittstelle 31

5.2.2 Sperren eines Zertifikats über den Sub-Registrator 39
5.2.3 Sperren eines Zertifikats über die Sperr-Hotline....39

5.3 Erneuern eines Zertifikats....40
5.3.1 Einsatz von Smartcards....40
5.3.2 Einsatz von Software-PSEs....44

5.4 Weitere Prozesse....56
5.4.1 Zertifikat suchen....57
5.4.2 Zertifikat prüfen....58
5.4.3 Sperrlisten abholen....59
5.4.4 Telekom Root laden....64
5.4.5 MailPass CA Zertifikat laden....66
5.4.6 Richtlinien laden....66

5.5 Export einer PKCS#12-Datei....66
5.5.1 Netscape Navigator....66
5.5.2 Microsoft Internet Explorer....68

5.6 Hinweise zum Einsatz des Internet Explorers....73

6 SICHERHEITSHINWEISE....78

6.1 Ihre Smartcard....78

6.2 Ihr Software-PSE....78

6.3 Weitere Richtlinien....80

7 PROBLEME UND LÖSUNGEN....81

GLOSSAR....83

1 EINLEITUNG

Viele Unternehmen und Organisationen nutzen heute die Vorteile, die sich aus Anwendungen wie dem Informationsaustausch mittels E-Mail, dem Dateitransfer oder Web-Services (zum Beispiel über Portale) ergeben. Die Vorteile, die mit der Nutzung elektronischer Medien einhergehen, werden häufig durch Gefahren und Einschränkungen gemindert oder gar aufgehoben. So wird geschäftliche Korrespondenz oft unverschlüsselt mittels E-Mail abgewickelt, Bestellungen werden nicht elektronisch signiert und Benutzer von Web-Seiten können nicht eindeutig identifiziert werden. Vergleicht man diese neuen elektronischen Geschäftsprozesse mit den konventionellen, werden die Risiken augenscheinlich: Niemand käme auf die Idee, Geschäftsbriefe in Klarsichthüllen oder auf Postkarten zu versenden. Eine Bestellung ohne Unterschrift und eindeutigen Absender würde wohl niemand bearbeiten.

Es ist daher erforderlich, Lösungen zu finden, welche die zentralen Sicherheitsziele eines Unternehmens für elektronische Geschäftsprozesse erfüllen:

- **Vertraulichkeit:** Daten sollen vor unberechtigter Einsichtnahme geschützt werden. Dies kann durch sichere Verschlüsselung erreicht werden.
- **Integrität:** Daten sollen vor Manipulation geschützt werden. Mit Hilfe digitaler Signaturen können Änderungen an Daten erkannt werden.
- **Authentizität:** Die Herkunft von Daten soll zweifelsfrei erkannt werden können. Mit Hilfe digitaler Signaturen können Daten bestimmten Personen zugeordnet werden. Ebenso können Personen beim Zugriff auf geschützte Web-Seiten identifiziert werden.

Mit dem Einsatz von Public-Key-Verfahren auf Basis digitaler Zertifikate können diese Ziele erreicht werden.

Mit T-TeleSec MailPass bietet die Deutsche Telekom die Infrastruktur und den Service für die Ausstellung und die Verwaltung entsprechender digitaler Zertifikate an.

Das vorliegende Handbuch wendet sich an die Benutzer des MailPass-Service der Deutschen Telekom TeleSec. Neben einer kurzen Einführung werden die dem Benutzer zur Verfügung stehenden Komponenten und deren Bedienung erläutert. Hauptbestandteil dieses Handbuchs ist eine detaillierte Beschreibung der vom Benutzer auszuführenden Aufgaben. Weitere Kapitel widmen sich Hinweisen zur Sicherheit sowie der Behandlung häufig auftretender Probleme.

2 PKI-GRUNDLAGEN

2.1 Schlüssel und Zertifikate

Für den sinnvollen Einsatz von Verschlüsselungs-, Signatur- und Authentifizierungsverfahren werden digitale Zertifikate benötigt. Ein **Zertifikat** ist eine Art elektronischer Ausweis, mit dem die Identität des Inhabers überprüft werden kann. Zertifikate kommen zum Beispiel zum Einsatz, wenn Sie Ihre E-Mails signieren, Dateien verschlüsseln oder sich an einem Web-Server gesichert anmelden

Grundlage für den Einsatz zertifikatsbasierter Verfahren ist ein Schlüsselpaar, bestehend aus einem privaten Schlüssel und einem öffentlichen Schlüssel. Diese beiden Schlüssel sind so voneinander abhängig, dass sie einander eindeutig zugeordnet werden können. Der private Schlüssel ist vom Besitzer unbedingt geheim zu halten. Der öffentliche Schlüssel hingegen muss dem Kommunikationspartner (im Fall von E-Mail-Verschlüsselung und -Signatur) bzw. dem Web-Server (im Fall einer Authentifizierung) bekannt gemacht werden. Für die Zuordnung des Schlüsselpaares zu einem Besitzer werden digitale Zertifikate verwendet. Diese enthalten neben dem Namen und dem öffentlichen Schlüssel des Besitzers einige weitere Angaben, wie beispielsweise eine Gültigkeitsdauer. Um die korrekte Zuordnung des Schlüssels zum Besitzer zu gewährleisten, werden solche Zertifikate von einer Zertifizierungsinstanz (CA) – einer Art elektronischer Ausweisbehörde – ausgestellt und signiert.

2.2 Das Trust Center und der Domain-Betreiber

Die Zertifizierungsinstanz, die Ihr Zertifikat ausstellt, heißt **MailPass CA** und wird von der Deutschen Telekom im **Telekom Trust Center** betrieben. Dies ist ein anerkanntes Trust Center mit langjährigen Erfahrungen im Bereich Zertifizierungsdienste. Qualifiziertes Personal sowie bauliche, technische und organisatorische Sicherheitsmaßnahmen sorgen dafür, dass Ihr Zertifikat höchsten Sicherheitsansprüchen genügt.

Die Organisation, welche den MailPass-Service des Telekom Trust Centers nutzt, wird als Domain-Betreiber bezeichnet. Der Domain-Betreiber ist also Ihr Unternehmen oder Ihre Behörde. Hier gibt es als Ansprechpartner einen MailPass-Verantwortlichen.

Bevor im Trust Center Ihr Zertifikat generiert wird, müssen Sie sich registrieren lassen. Dadurch wird verhindert, dass eine unberechtigte Person ein Zertifikat in Ihrem Namen erhält. Die Registrierung wird von einem Mitarbeiter des Domain-Betreibers, dem so genannten Sub-Registrator, durchgeführt. Hierfür gibt es zwei Möglichkeiten: Bei einer **zentralen Registrierung** werden Sie persönlich von dem Sub-Registrator anhand von Ausweisdokumenten identifiziert. Danach sendet der Sub-Registrator Ihren Zertifikatsantrag an das Trust Center. Falls Sie dem Sub-Registrator schon bekannt sind, zum Beispiel anhand bereits erfasster Personaldaten, kann auch eine **dezentrale Registrierung** durchgeführt werden. In diesem Fall stellen Sie selbst den Zertifikatsantrag an das Trust Center. Der Sub-Registrator braucht dann nur noch dem Trust Center bestätigen, dass Sie berechtigt sind, dieses Zertifikat zu erhalten. Welche dieser Registrierungsmöglichkeiten für Sie in Frage kommt, teilt Ihnen Ihr MailPass-Verantwortlicher mit.

2.3 Smartcards und Software-PSEs

Das Sicherheitsniveau der MailPass-Zertifikate hängt nicht nur von den Sicherheitsmaßnahmen des Trust Centers und der Registrierung der Zertifikatsinhaber ab. Ein wesentlicher Punkt ist die Geheimhaltung des privaten Schlüssels. Hierfür wird dieser in einem speziell gesicherten Bereich gespeichert. Eine Möglichkeit hierfür sind Software-PSEs. Ein Software-PSE ist eine verschlüsselte passwortgeschützte Datei. Um einen maximalen Schutz des privaten Schlüssels zu gewährleisten, sollte dieser jedoch auf einer Smartcard gespeichert werden.

Abbildung 1: Eine Smartcard ist an einer Kontaktfläche aus Metall zu erkennen.

Eine Smartcard ist eine Plastikkarte im Scheckkartenformat auf der ein Computerchip angebracht ist. Dieser Computerchip ist an einer Kontaktfläche aus Metall zu erkennen. Der Chip einer Smartcard ist ein Computer im Kleinformat, der – wie ein größerer Computer auch – Daten speichern und mit ihnen rechnen kann. Eine Smartcard eignet sich hervorragend, um darauf einen privaten Schlüssel zu speichern, der anschließend nicht mehr auslesbar ist. Auch die Rechenoperationen, für die der private Schlüssel benötigt wird, lassen sich auf dem Chip durchführen. Die Verwendung von Smartcards ist somit eine besonders sichere Form der Schlüsselspeicherung, da der Schlüssel nur einmal existiert, nicht kopiert werden kann und die Karte nicht verlässt.

Die Deutsche Telekom stellt im Rahmen des MailPass-Services NetKey E4 Smartcards zur Verfügung. Diese sind von unabhängigen Stellen geprüft und genügen höchsten Sicherheitsanforderungen.

2.4 Single Key / Dual Key

Beim Anlegen eines Zuständigkeitsbereichs (Sub-Domain) wird festgelegt, ob die Benutzer dieses Zuständigkeitsbereichs Dual Key oder Single Key verwenden.

Wenn für Ihren Zuständigkeitsbereich **Single Key** konfiguriert wurde, verwenden Sie **ein** Schlüsselpaar. Für dieses erhalten Sie **ein** Zertifikat. Das Zertifikat können Sie sowohl zur Signatur als auch für Verschlüsselung einsetzen.

Wenn für Ihren Zuständigkeitsbereich **Dual Key** konfiguriert wurde, verwenden Sie **zwei getrennte** Schlüsselpaare. Für **jedes** erhalten Sie **ein** Zertifikat. Sie haben also zwei Zertifikate für verschiedene Verwendungszwecke – je eins für Signatur und Verschlüsselung. Die Verwaltung der beiden Zertifikate erfolgt synchron: Sie werden gemeinsam beantragt, bei (vorläufiger) Sperrung des einen Zertifikats erfolgt automatisch auch die (vorläufige) Sperrung des anderen Zertifikats und auch die Erneuerung erfolgt nur für beide Zertifikate zusammen.

3 AUFGABEN DES BENUTZERS

Als Benutzer sind Sie verantwortlich für verschiedene Aufgaben im Umgang mit Ihrem Zertifikat. Dies beinhaltet insbesondere die Beantragung, die Sperrung und die Erneuerung Ihres Zertifikats. Wie Sie diese Aufgaben wahrnehmen können und welche Komponenten Ihnen dafür zur Verfügung stehen, ist in den Kapiteln 4 und 5 beschrieben.

Das Sicherheitsniveau hängt auch wesentlich von der Sorgfalt beim Umgang mit Ihrem privaten Schlüssel ab. Kapitel 6 enthält einige Hinweise, die Sie zur Gewährleistung eines hohen Sicherheitsniveaus beachten müssen.

4 KOMPONENTEN

Für die Aufgaben, welche Sie im Umgang mit Ihrem Zertifikat haben, stehen Ihnen verschiedene Komponenten zur Verfügung. Je nach dem von Ihrem Domain-Betreiber gewählten Registrierungsmodell steht Ihnen die Benutzer-Web-Schnittstelle oder die eingeschränkte Benutzer-Web-Schnittstelle zur Verfügung. Dies sind Web-Seiten, auf denen Sie wichtige Funktionen rund um Ihr Zertifikat finden. Weiterhin besteht die Möglichkeit, über die Mail-Request-Schnittstelle Zertifikate zu beantragen. Die LDAP-Schnittstelle bietet Ihnen die Möglichkeit, Zertifikate und Sperrlisten vom Verzeichnisdienst abzurufen. Die OCSP-Schnittstelle bietet Ihnen die Möglichkeit, Zertifikate online zu prüfen.

Bei Ihrem Domain-Betreiber gibt es außerdem einen Sub-Registrator, welcher für das Management Ihres Zertifikats verantwortlich ist. Auch über diesen können Sie verschiedene Aktionen veranlassen. Für Notfälle gibt es eine Hotline, über die Sie Ihr Zertifikat sperren lassen können. Für weitere Fragen steht Ihnen ein MailPass-Verantwortlicher des Domain-Betreibers zur Verfügung. Die einzelnen Komponenten werden in diesem Kapitel beschrieben.

4.1 Voraussetzungen

Um die Web-Schnittstellen für die Zertifikatsdienste von T-TeleSec MailPass nutzen zu können, muss Ihr Arbeitsplatz folgende Voraussetzungen erfüllen:

- Web-Browser
- Smartcard-Leser (nur, wenn Smartcards zum Einsatz kommen)
- E-Mail-Account

Genaue Informationen zu den eingesetzten Produkten erfahren Sie von Ihrem MailPass-Verantwortlichen.

4.2 Benutzer-Web-Schnittstelle

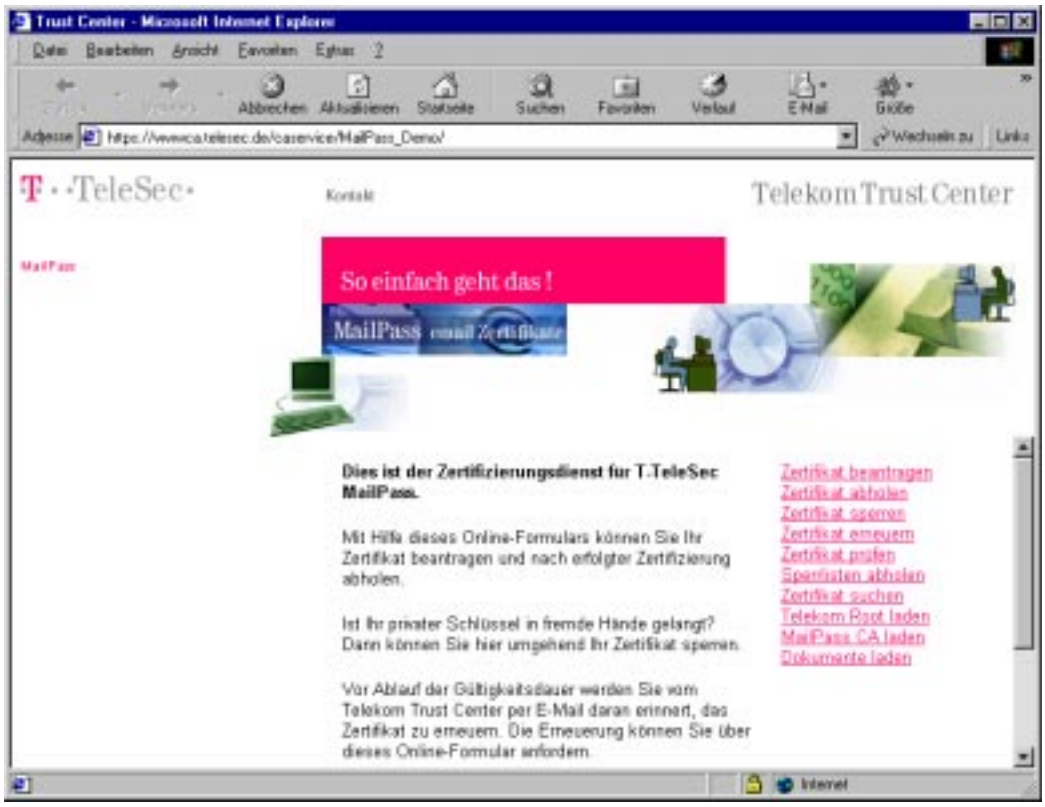
Trust Center - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Größe
Adresse https://www.ca.telesec.de/caservice/MailPass_Demo/
Wechseln zu Links
T · TeleSec
Kontakt
Telekom Trust Center
MailPass
So einfach geht das !
MailPass email Zertifikate
Dies ist der Zertifizierungsdienst für T-TeleSec MailPass.
Mit Hilfe dieses Online-Formulars können Sie Ihr Zertifikat beantragen und nach erfolgter Zertifizierung abholen.
Ist Ihr privater Schlüssel in fremde Hände gelangt? Dann können Sie hier umgehend Ihr Zertifikat sperren.
Vor Ablauf der Gültigkeitsdauer werden Sie vom Telekom Trust Center per E-Mail daran erinnert, das Zertifikat zu erneuern. Die Erneuerung können Sie über dieses Online-Formular anfordern.
Zertifikat beantragen
Zertifikat abholen
Zertifikat sperren
Zertifikat erneuern
Zertifikat prüfen
Sperrlisten abholen
Zertifikat suchen
Telekom Root laden
MailPass CA laden
Dokumente laden
Internet

Abbildung 2: Startseite der Benutzer-Web-Schnittstelle

Die Benutzer-Web-Schnittstelle steht Ihnen zur Verfügung, wenn Ihr Domain-Betreiber das dezentrale Registrierungsmodell gewählt hat. Diese Komponente können Sie mit Ihrem Browser aufrufen. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Die erforderlichen Daten können Sie dem Informationsblatt entnehmen, welches Ihnen Ihr MailPass-Verantwortlicher übergeben hat.

Auf diesen Web-Seiten stehen Ihnen folgende Funktionen zur Verfügung:

- **Zertifikat beantragen:** Mit Hilfe dieses Online-Formulars können Sie Ihr persönliches Zertifikat beantragen.
- **Zertifikat abholen:** Nach erfolgter Zertifizierung werden Sie vom Telekom Trust Center per E-Mail darüber informiert, dass Sie Ihr Zertifikat abholen können. Dafür steht Ihnen diese Funktion zur Verfügung.
- **Zertifikat sperren:** Wenn Ihr privater Schlüssel in falsche Hände gelangt ist oder ein anderer wichtiger Grund vorliegt, können Sie über diesen Menüpunkt die Sperrung Ihres Zertifikats veranlassen.
- **Zertifikat erneuern:** Ihr Zertifikat hat eine begrenzte Gültigkeitsdauer. Bevor diese abläuft, werden Sie vom Telekom Trust Center per E-Mail daran erinnert, das Zertifikat zu erneuern. Die Erneuerung können Sie über dieses Online-Formular anfordern.
- **Zertifikat prüfen:** Hier können Sie prüfen, ob Ihr Zertifikat gültig ist.
- **Sperrlisten abholen:** Die Sperrung von Zertifikaten wird über eine Sperrliste bekannt gemacht. Mit dieser Funktion können Sie eine aktuelle Liste der gesperrten Benutzerzertifikate (CRL,

Certificate Revocation List) bzw. der gesperrten CA-Zertifikate (ARL, Authority Revocation List) anfordern.

- **Zertifikat suchen:** Hier können Sie ein Zertifikat im Verzeichnisdienst suchen. Ist das Verzeichnis zugriffsgeschützt, müssen Sie einen Benutzernamen und ein Passwort angeben. Diese Daten erhalten Sie von Ihrem MailPass-Verantwortlichen.
- **Telekom Root laden:** Hier können Sie das Zertifikat der Zertifizierungsinstanz laden, welche das MailPass CA Zertifikat ausgestellt hat.
- **MailPassPass CA laden:** Hier können Sie das Zertifikat der Zertifizierungsinstanz laden, welche Ihr Zertifikat ausstellt.
- **Dokumente laden:** Hier steht Ihnen ein Dokument mit den Zertifizierungsrichtlinien (CPS) der Deutschen Telekom für den MailPass-Service sowie das Benutzerhandbuch zur Verfügung.

4.3 Eingeschränkte Benutzer-Web-Schnittstelle

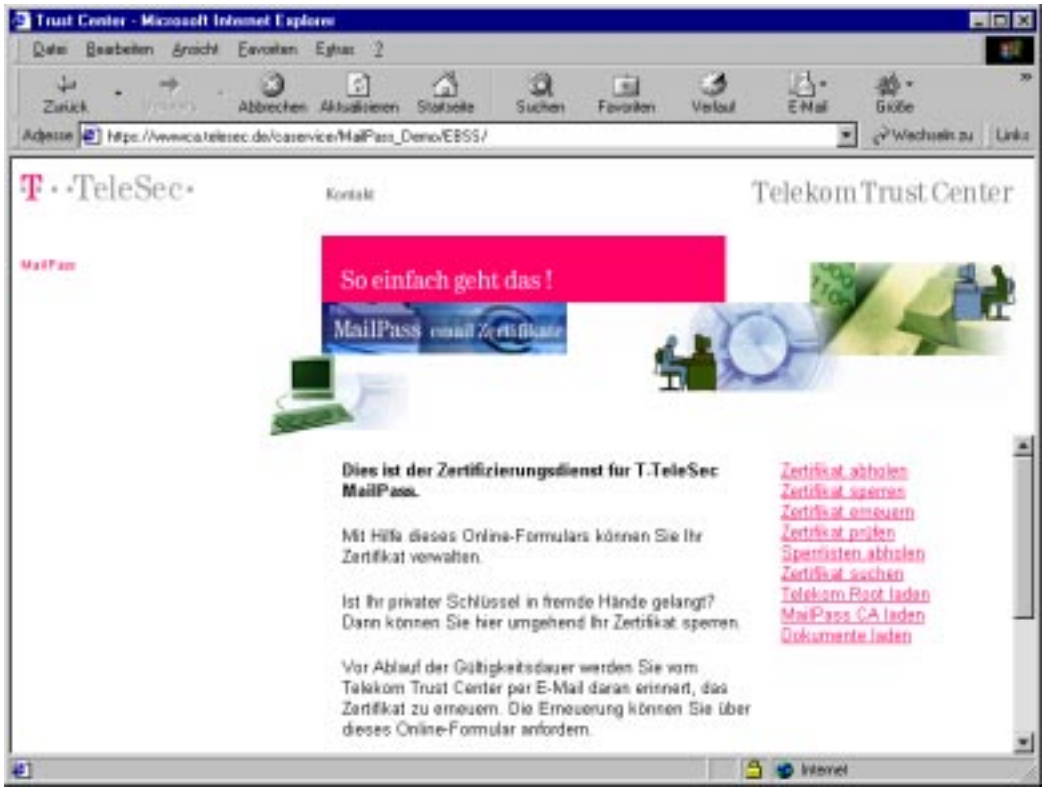
Trust Center - Microsoft Internet Explorer
TeleSec
Telekom Trust Center
So einfach geht das !
MailPass
Dies ist der Zertifizierungsdienst für T.TeleSec MailPass.
Mit Hilfe dieses Online-Formulars können Sie Ihr Zertifikat verwalten.
Ist Ihr privater Schlüssel in fremde Hände gelangt? Dann können Sie hier umgehend Ihr Zertifikat sperren.
Vor Ablauf der Gültigkeitsdauer werden Sie vom Telekom Trust Center per E-Mail daran erinnert, das Zertifikat zu erneuern. Die Erneuerung können Sie über dieses Online-Formular anfordern.
Zertifikat abholen
Zertifikat sperren
Zertifikat erneuern
Zertifikat prüfen
Sperrlisten abholen
Zertifikat suchen
Telekom Root laden
MailPass CA laden
Dokumente laden

Abbildung 3: Startseite der eingeschränkten Benutzer-Web-Schnittstelle

Die eingeschränkte Benutzer-Web-Schnittstelle steht Ihnen zur Verfügung, wenn Ihr Domain-Betreiber das zentrale Registrierungsmodell gewählt hat. Diese Komponente können Sie mit Ihrem Browser aufrufen. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Die erforderlichen Daten können Sie dem Informationsblatt entnehmen, welches Ihnen der Sub-Registrator übergeben hat.

Auf diesen Web-Seiten stehen Ihnen folgende Funktionen zur Verfügung:

- **Zertifikat abholen:** Nach erfolgter Zertifikatserneuerung werden Sie vom Telekom Trust Center per E-Mail darüber informiert, dass Sie Ihr Zertifikat abholen können. Dafür steht Ihnen diese Funktion zur Verfügung.
- **Zertifikat sperren:** Wenn Ihr privater Schlüssel in falsche Hände gelangt ist oder ein anderer wichtiger Grund vorliegt, können Sie über diesen Menüpunkt die Sperrung Ihres Zertifikats veranlassen.
- **Zertifikat erneuern:** Ihr Zertifikat hat eine begrenzte Gültigkeitsdauer. Bevor diese abläuft werden Sie vom Telekom Trust Center per E-Mail daran erinnert, das Zertifikat zu erneuern. Die Erneuerung können Sie über dieses Online-Formular anfordern.
- **Zertifikat prüfen:** Hier können Sie prüfen, ob Ihr Zertifikat gültig ist.
- **Sperrlisten abholen:** Die Sperrung von Zertifikaten wird über eine Sperrliste bekannt gemacht. Mit dieser Funktion können Sie eine aktuelle Liste der gesperrten Benutzerzertifikate (CRL, Certificate Revocation List) bzw. der gesperrten CA-Zertifikate (ARL, Authority Revocation List) anfordern.
- **Zertifikat suchen:** Hier können Sie ein Zertifikat im Verzeichnisdienst suchen. Ist das Verzeichnis zugriffsgeschützt, müssen Sie einen Benutzernamen und ein Passwort angeben. Diese Daten erhalten Sie von Ihrem MailPass-Verantwortlichen.
- **Telekom Root laden:** Hier können Sie das Zertifikat der Zertifizierungsinstanz laden, welche das MailPass CA Zertifikat ausgestellt hat.
- **MailPass CA laden:** Hier können Sie das Zertifikat der Zertifizierungsinstanz laden, welche Ihr Zertifikat ausstellt.
- **Dokumente laden:** Hier steht Ihnen ein Dokument mit den Zertifizierungsrichtlinien (CPS) der Deutschen Telekom für den MailPass-Service sowie das Benutzerhandbuch zur Verfügung.

4.4 Mail-Request-Schnittstelle

Die Mail-Request-Schnittstelle erlaubt Ihnen die dezentrale Registrierung per E-Mail. Zu diesem Zweck müssen Sie zunächst mit einer geeigneten Client-Anwendung einen Zertifikatsantrag im Format PKCS#10 erzeugen. Diesen schicken Sie dann per E-Mail an das Telekom Trust Center. Die E-Mail-Adresse erhalten Sie von Ihrem MailPass-Verantwortlichen. Anschließend nehmen Sie Kontakt mit Ihrem Sub-Registrator auf und handeln ein Sperrpasswort aus. Bei erfolgreicher Bearbeitung Ihres Antrags wird Ihnen dann das Zertifikat direkt per E-Mail zugeschickt.

4.5 LDAP-Schnittstelle

Es besteht die Möglichkeit, mit einem LDAP-fähigen Client (zum Beispiel einer geeigneten E-Mail-Lösung) Zertifikate und Sperrlisten über das LDAP-Protokoll vom Verzeichnisdienst direkt abzurufen. Weitere Informationen zu dieser Schnittstelle erhalten Sie von Ihrem MailPass-Verantwortlichen.

4.6 OCSP-Schnittstelle

Mittels OCSP (Online Certificate Status Protocol) kann eine entsprechende Client-Anwendung, die dieses Protokoll unterstützt, den Status von Zertifikaten online prüfen.
Weitere Informationen zu dieser Schnittstelle erhalten Sie von Ihrem MailPass-Verantwortlichen.

4.7 Sub-Registrator

Bei Ihrem Domain-Betreiber gibt es einen Sub-Registrator, welcher für das Management Ihres Zertifikats verantwortlich ist. Er nimmt folgende Aufgaben wahr:

- **Zertifikat beantragen:** Im Falle des zentralen Registrierungsmodells müssen Sie beim Sub-Registrator vorstellig werden, um Ihr Zertifikat zu beantragen.
- **Zertifikatsanträge bearbeiten:** Wenn Ihr Domain-Betreiber das dezentrale Registrierungsmodell gewählt hat, bearbeitet der Sub-Registrator Ihren Zertifikatsantrag.
- **Vorläufige Zertifikatssperrungen bearbeiten:** Wenn Sie eine Zertifikatssperrung über die Sperr-Hotline beantragt haben, muss diese durch den Sub-Registrator bearbeitet werden.
- **Zertifikat sperren:** Sie können beim Sub-Registrator per E-Mail (oder ggf. auch telefonisch oder persönlich) die Sperrung Ihres Zertifikats anfordern. Die E-Mail-Adresse und Telefonnummer entnehmen Sie bitte dem bei der Registrierung erhaltenen Informationsblatt.

4.8 Zentrale Sperr-Hotline

Falls es Ihnen nicht möglich ist, Ihr Zertifikat über die Benutzer-Web-Schnittstelle bzw. die eingeschränkte Benutzer-Web-Schnittstelle oder über den Sub-Registrator zu sperren, können Sie die Sperrung auch über eine Sperr-Hotline veranlassen. Die Nummer dieser Hotline entnehmen Sie bitte dem Informationsblatt, welches Sie bei der Registrierung erhalten haben.

4.9 MailPass-Verantwortlicher

Der MailPass-Verantwortliche Ihres Domain-Betreibers ist Ihr Ansprechpartner für MailPass-spezifische Probleme.

5 PROZESSE

5.1 Beantragen eines Zertifikats

Wenn Sie ein Zertifikat beantragen wollen, müssen Sie von Ihrem Domain-Betreiber registriert werden. Hierfür gibt es zwei verschiedene Abläufe:

- **Zentrale Registrierung:** Um ein Zertifikat zu erhalten, müssen Sie persönlich von einem Sub-Registrator registriert werden.
- **Dezentrale Registrierung:** Sie können einen Online-Zertifikatsantrag über die Web- oder Mail-Request-Schnittstelle stellen. Dieser wird dann durch einen Sub-Registrator bearbeitet.

Eine weitere Unterscheidung der Abläufe ergibt sich durch den Einsatz von Smartcards oder Software-PSEs als Speichermedium für das Zertifikat und den privaten Schlüssel. Insgesamt gibt es also für das Beantragen Ihres Zertifikats folgende Alternativen:

- Zentrale Registrierung beim Einsatz von Smartcards
- Zentrale Registrierung beim Einsatz von Software-PSEs
- Dezentrale Registrierung über die Web-Schnittstelle beim Einsatz von Smartcards
- Dezentrale Registrierung über die Web-Schnittstelle beim Einsatz von Software-PSEs
- Dezentrale Registrierung über die Mail-Request-Schnittstelle beim Einsatz von Smartcards
- Dezentrale Registrierung über die Mail-Request-Schnittstelle beim Einsatz von Software-PSEs

Für welche dieser Alternativen sich Ihr Domain-Betreiber entschieden hat und welche der im Folgenden beschriebenen Abläufe für Sie maßgeblich sind, teilt Ihnen Ihr MailPass-Verantwortlicher mit.

5.1.1 Zentrale Registrierung beim Einsatz von Smartcards

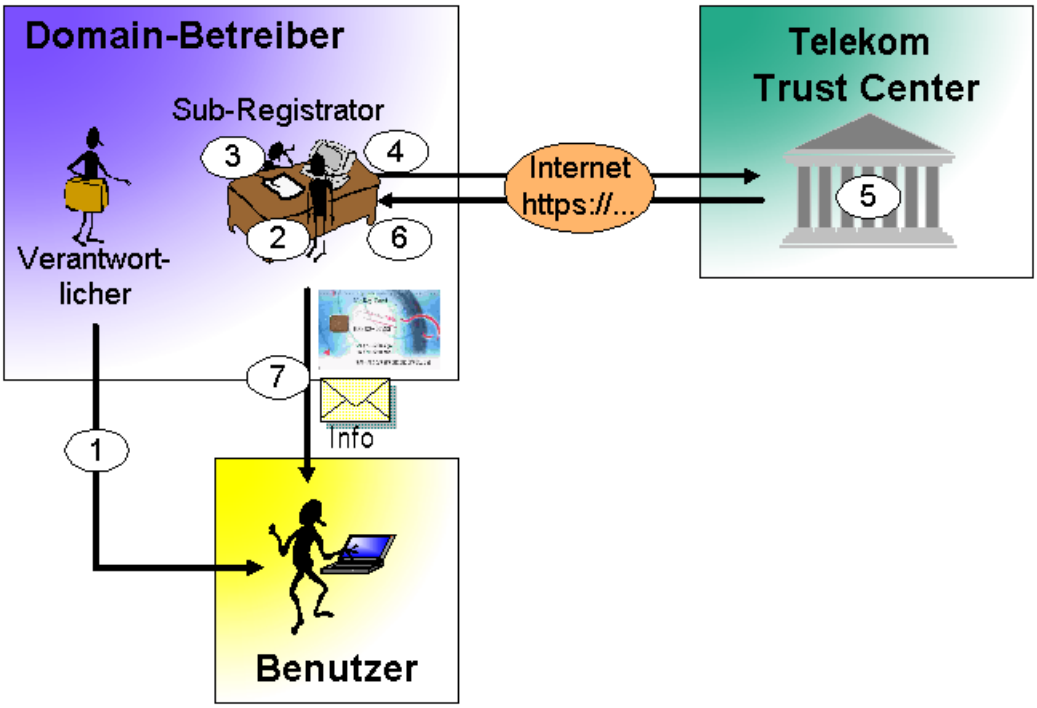

Abbildung 4: Beantragung eines Benutzerzertifikats mit Smartcard bei zentraler Registrierung

Abbildung 4 verdeutlicht den Ablauf der Beantragung Ihres Zertifikats. Es müssen folgende Schritte ausgeführt werden:

1) Sie werden vom MailPass-Verantwortlichen benachrichtigt, dass Sie ein Zertifikat beantragen können. Dabei wird Ihnen der verantwortliche Sub-Registrator genannt.
2) Sie müssen persönlich beim Sub-Registrator erscheinen. Dort wird Ihre Identität anhand eines Ausweisdokuments geprüft. Außerdem prüft der Sub-Registrator Ihre Berechtigung zur Zertifikatsbeantragung anhand einer ihm vorliegenden Liste.
3) Der Sub-Registrator füllt den Zertifikatsantrag über ein Web-Formular aus. Dabei legen Sie ein Sperrpasswort fest, welches mit in den Antrag eingeht. Dieses müssen Sie sich gut merken, da es abgefragt wird, wenn Sie Ihr Zertifikat sperren lassen.
4) Beim Absenden des Zertifikatsantrags müssen Sie die PIN für Ihre Smartcard festlegen und am Smartcard-Leser eingeben. Die PIN muss sechsstellig sein. Diese PIN müssen Sie sich gut merken, da sie bei jeder Benutzung der Smartcard abgefragt wird.
5) Im Telekom Trust Center wird Ihr Zertifikat erzeugt und in einem Verzeichnisdienst gespeichert.
6) Der Sub-Registrator lädt das Zertifikat auf Ihre Smartcard. Dabei müssen Sie Ihre PIN am Smartcard-Leser eingeben.
7) Der Sub-Registrator übergibt Ihnen die Smartcard und ein Informationsblatt. Dieses enthält:
   - die Web-Adresse der eingeschränkten Benutzer-Web-Schnittstelle, über die Sie Ihr Zertifikat sperren und erneuern können sowie einen dazugehörigen Benutzernamen und ein Passwort,
   - die E-Mail-Adresse und ggf. eine Telefonnummer des Sub-Registrators, über den Sie die Sperrung Ihres Zertifikats veranlassen können und
   - die Telefonnummer der Sperr-Hotline, über die Sie die Sperrung Ihres Zertifikats veranlassen können.

5.1.2 Zentrale Registrierung beim Einsatz von Software-PSEs

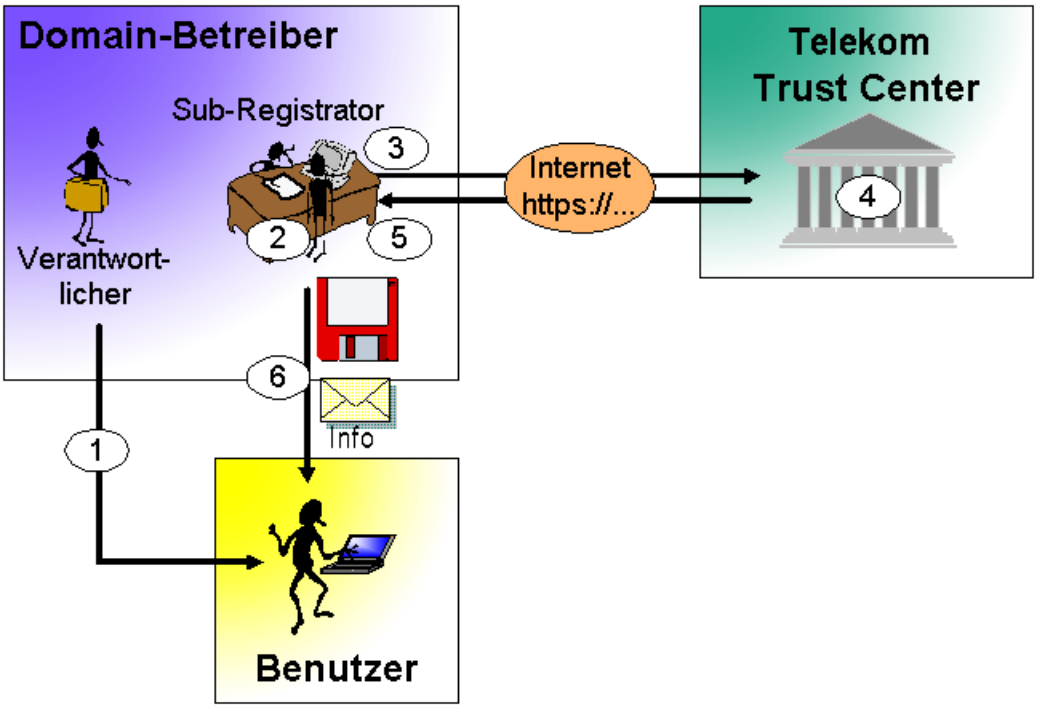

Abbildung 5: Beantragung eines Benutzerzertifikats mit Software-PSE bei zentraler Registrierung

Abbildung 5 verdeutlicht den Ablauf der Beantragung Ihres Zertifikats. Es müssen folgende Schritte ausgeführt werden:

1) Sie werden vom MailPass-Verantwortlichen benachrichtigt, dass Sie ein Zertifikat beantragen können. Dabei wird Ihnen der verantwortliche Sub-Registrator genannt.
2) Sie müssen persönlich beim Sub-Registrator erscheinen. Dort wird Ihre Identität anhand eines Ausweisdokuments geprüft. Außerdem prüft der Sub-Registrator Ihre Berechtigung zur Zertifikatsbeantragung anhand einer ihm vorliegenden Liste.
3) Der Sub-Registrator füllt den Zertifikatsantrag über ein Web-Formular aus und sendet ihn anschließend an das Trust Center ab. Dabei legen Sie ein Sperrpasswort fest. Dieses müssen Sie sich gut merken, da es abgefragt wird, wenn Sie Ihr Zertifikat sperren lassen.
4) Im Telekom Trust Center wird Ihr Zertifikat erzeugt und in einem Verzeichnisdienst gespeichert.
5) Der Sub-Registrator speichert Ihr Zertifikat und den privaten Schlüssel in einer Datei (*.p12) auf einer Diskette. Die Datei ist mit einem Passwort geschützt, welches Sie festlegen und eingeben müssen (beachten Sie dabei bitte die Hinweise in Kapitel 6.2). Dieses Passwort müssen Sie sich gut merken, da es beim Import Ihres privaten Schlüssels und des Zertifikats in ihre Client-Software abgefragt wird und Sie es auch später noch benötigen.
6) Der Sub-Registrator übergibt Ihnen die Diskette und ein Informationsblatt. Dieses enthält:
   - die Web-Adresse der eingeschränkten Benutzer-Web-Schnittstelle, über die Sie Ihr Zertifikat sperren und erneuern können sowie einen dazugehörigen Benutzernamen und ein Passwort,
   - die E-Mail-Adresse und ggf. die Telefonnummer des Sub-Registrators, über den Sie die Sperrung Ihres Zertifikats veranlassen können und
   - die Nummer der Sperr-Hotline, über die Sie die Sperrung Ihres Zertifikats veranlassen können.

5.1.3 Dezentrale Registrierung über die Web-Schnittstelle beim Einsatz von Smartcards

Hinweis: *Wenn Sie die Beantragung mit dem Netscape Navigator durchführen, müssen Sie zunächst sicherstellen, dass die Communicator-Datenbank mit einem Passwort geschützt ist.*

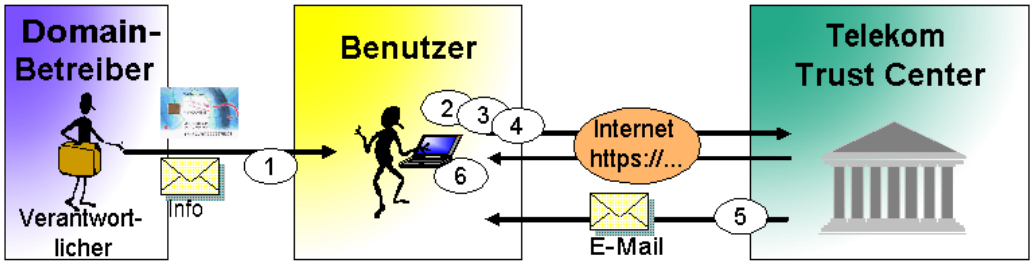

Abbildung 6: Beantragung eines Benutzerzertifikats über Web-Schnittstelle mit Smartcard bei dezentraler Registrierung

Abbildung 6 verdeutlicht den Ablauf der Beantragung Ihres Zertifikats. Es müssen folgende Schritte ausgeführt werden:

1) Sie werden vom MailPass-Verantwortlichen benachrichtigt, dass Sie ein Zertifikat beantragen können. Dabei wird Ihnen eine NetKey Smartcard übergeben. Außerdem erhalten Sie ein Informationsblatt. Dieses enthält:
   - die Web-Adresse der Benutzer-Web-Schnittstelle, über die Sie Ihr Zertifikat beantragen, sperren und erneuern können sowie einen dazugehörigen Benutzernamen und ein Passwort,
   - die E-Mail-Adresse und ggf. die Telefonnummer des Sub-Registrators, über den Sie die Sperrung Ihres Zertifikats veranlassen können,
   - die Nummer der Sperr-Hotline, über die Sie die Sperrung Ihres Zertifikats veranlassen können und
   - Vorgaben zum Ausfüllen des Zertifikatsantrags.
2) Sie rufen mit Ihrem Browser die Web-Seite der Benutzer-Web-Schnittstelle auf. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Diese Daten können Sie dem Informationsblatt entnehmen, welches Ihnen der MailPass-Verantwortliche übergeben hat.

Abbildung 7: Anmeldung mit Benutzername und zugehörigem Passwort

3) Wählen Sie die Funktion *Zertifikat beantragen*. Nun müssen Sie zunächst den Zuständigkeitsbereich auswählen, der Ihnen mitgeteilt wurde.

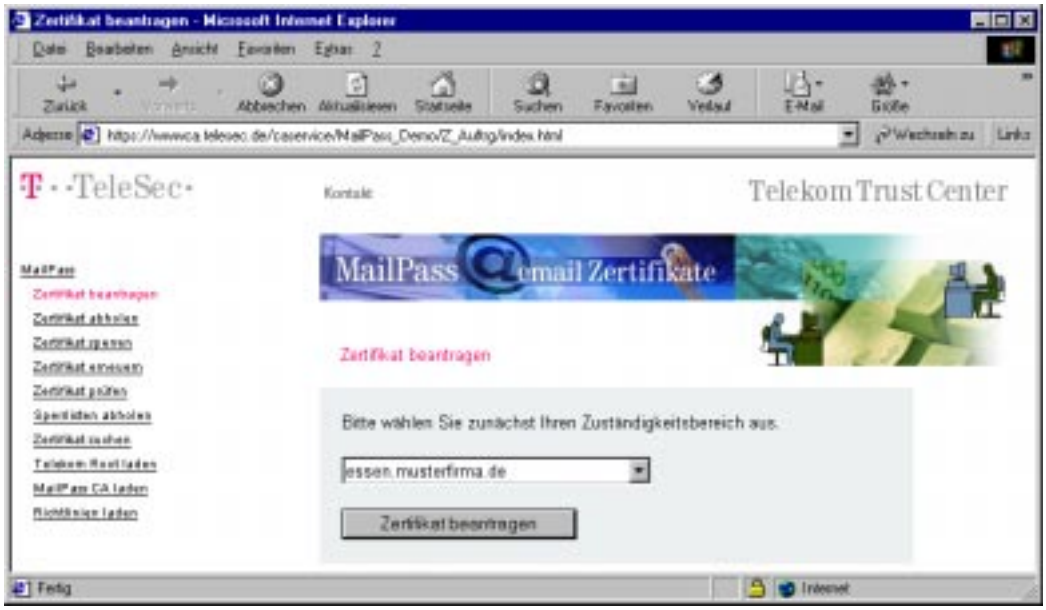

Abbildung 8: Auswählen des Zuständigkeitsbereichs

4) Nach Auswahl des Zuständigkeitsbereiches erscheint ein Online-Formular.

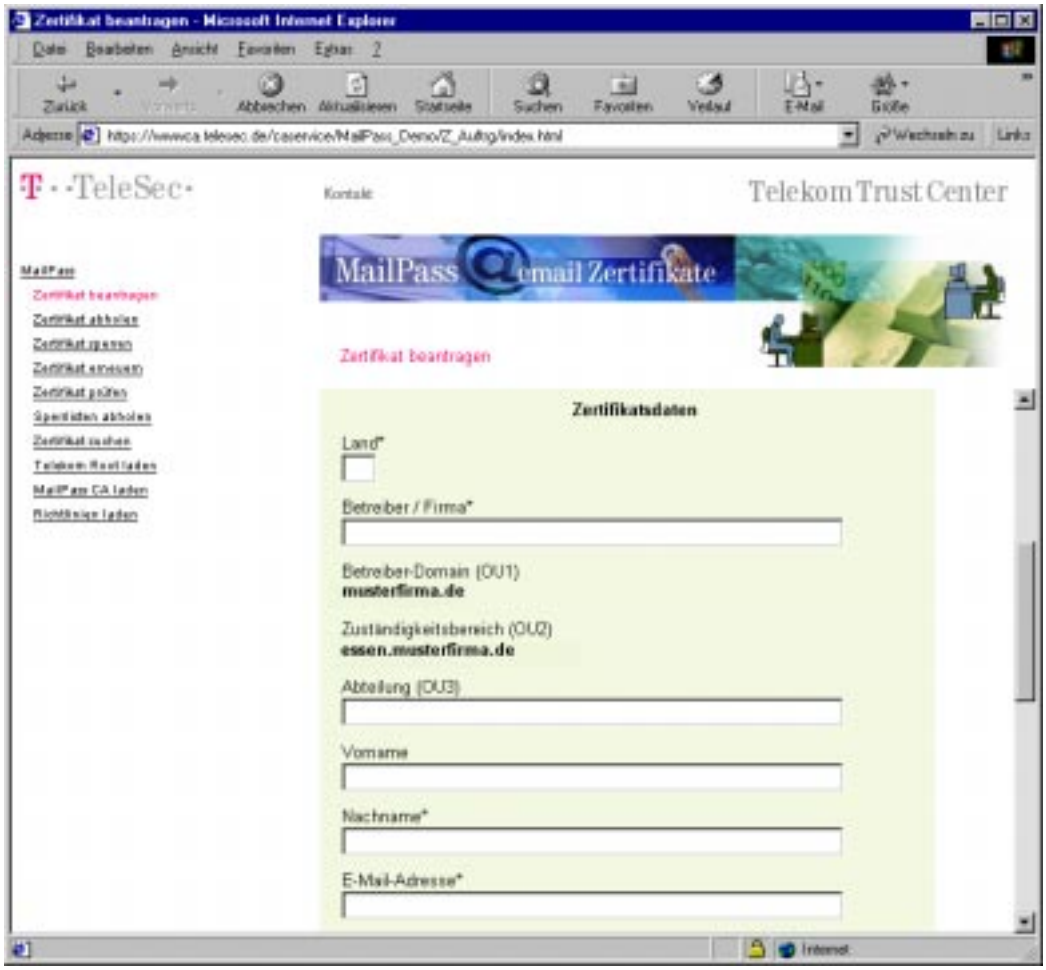

Abbildung 9: Antrag für Benutzerzertifikat

Gehen Sie bitte wie folgt vor:

a) Stecken Sie Ihre Smartcard in den Smartcard-Leser ein.

b) Füllen Sie die Datenfelder aus. Beachten Sie dabei bitte die Vorgaben ihres MailPass-Verantwortlichen. Beachten Sie des Weiteren, dass Vor- und Nachname keine Umlaute enthalten dürfen. Gültige Zeichen sind: *a-z A-Z 0-9 ' ( ) + , . / : ? = -*

c) Tragen Sie die Authentifizierungsdaten ein. Von besonderer Wichtigkeit ist das Sperrpasswort. Dieses müssen Sie sich gut merken, da es abgefragt wird, wenn Sie Ihr Zertifikat sperren lassen.

d) Für das Feld zur Auswahl des Schlüsselgenerators wählen Sie bitte folgende Einstellungen:
   - Netscape Navigator: *1024 (Verschlüsselung hoher Komplexität)*

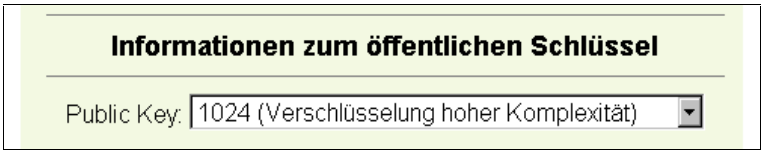

Abbildung 10: Einstellen der Schlüssellänge (Netscape)

   - MS Internet Explorer: *Kobil Smart CSP*

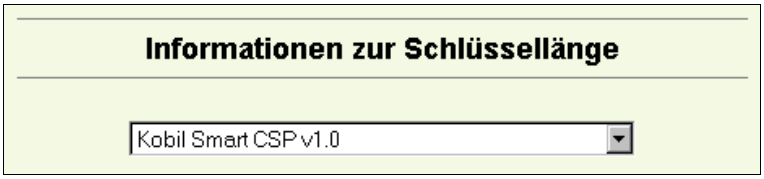

Abbildung 11: Auswahl der Smartcard zur Schlüsselgenerierung (Internet Explorer)

e) Klicken Sie auf den Button *Absenden*.
Wenn Sie den Netscape Navigator verwenden, erscheint ein neues Fenster, in dem Sie die Smartcard auswählen müssen (siehe Abbildung 12).

Private Key erstellen - Netscape
Private Key erstellen
Klicken Sie auf "OK". Für Ihr Zertifikat wird nun ein Private Key erstellt
Dies kann einige Minuten dauern.
Wichtig: Wird dieser Vorgang unterbrochen, müssen Sie das Zertifikat erneut anfordern.
Wählen Sie die Karte oder Datenbank, mit der der Schlüssel generiert werden soll:
TCOS 2.0 Chipkarte an COM 1
Mehr Info...
OK
Abbrechen

Abbildung 12: Bei Verwendung des Netscape Navigators muss die Smartcard zur Schlüsselgenerierung ausgewählt werden.

f) Beim Absenden des Zertifikatsantrages müssen Sie die PIN ihrer Smartcard eingeben. Bei erstmaliger Verwendung der Smartcard wird der Null-PIN-Status aufgehoben und Sie müssen eine neue sechsstellige PIN setzen. Abbildung 13 zeigt diesen Vorgang für den Internet Explorer. Bei Verwendung von Netscape erscheinen dazu zwei Fenster, wobei Sie ersteres ohne Eingabe durch Klicken von *OK* übergehen können (Abbildung 14). Im zweiten Fenster legen Sie Ihre neue PIN fest (Abbildung 15). Die Dialoge unterscheiden sich in Ihrem Aussehen je nach verwendeten Browser.

Abbildung 13: Geben Sie die gewünschte PIN ein (Internet Explorer)

Communicator-Kennwort einrichten - Netscape
Communicator-Kennwort einrichten
TCOS 2.0 Chipkarte an COM 1 wurde nicht mit einer Kennummer bzw. einem Kennwort initialisiert. Zum Initialisieren dieser Karte muß zunächst das Kennwort für den Netsite-Verwalter oder die -Sicherheit eingegeben werden. Kennen Sie das Kennwort nicht, klicken Sie auf Abbrechen, und geben Sie die Karte dem Aussteller zurück, um sie initialisieren zu lassen.
Verwaltungskennwort eingeben für TCOS 2.0 Chipkarte an COM 1:
OK
Abbrechen

Abbildung 14: Dieses Fenster können Sie ohne Eingabe durch Klicken von *OK* bestätigen (Netscape)

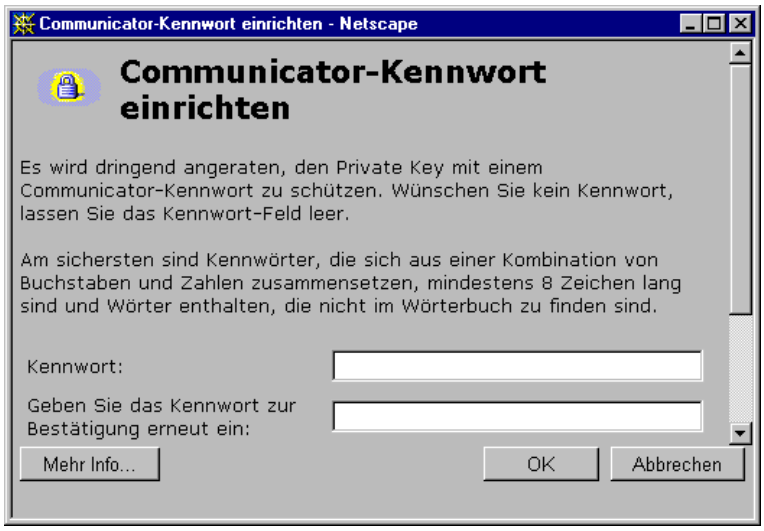
Communicator-Kennwort einrichten - Netscape
Communicator-Kennwort einrichten
Es wird dringend angeraten, den Private Key mit einem Communicator-Kennwort zu schützen. Wünschen Sie kein Kennwort, lassen Sie das Kennwort-Feld leer.
Am sichersten sind Kennwörter, die sich aus einer Kombination von Buchstaben und Zahlen zusammensetzen, mindestens 8 Zeichen lang sind und Wörter enthalten, die nicht im Wörterbuch zu finden sind.
Kennwort:
Geben Sie das Kennwort zur Bestätigung erneut ein:
Mehr Info...
OK
Abbrechen

Abbildung 15: Geben Sie die gewünschte PIN ein (Netscape)

g) Auf der Antwortseite in Ihrem Browser wird die Referenznummer Ihres Zertifikatsantrags angezeigt. Nach dem Erscheinen der Antwortseite in Ihrem Browser können Sie die Smartcard aus dem Smartcard-Leser entnehmen.

5) Nach der Erzeugung Ihres Zertifikats im Telekom Trust Center werden Sie per E-Mail benachrichtigt. Die E-Mail enthält die Referenznummer Ihres Antrags und die Web-Adresse, über die Sie Ihr Zertifikat abholen können.

6) Sie rufen mit Ihrem Browser die in der E-Mail angegebene Web-Seite auf. Alternativ können Sie auch über die Benutzer-Web-Schnittstelle die Funktion *Zertifikat abholen* aufrufen.

a) Tragen Sie die Referenznummer Ihres Zertifikatantrags in das vorgesehene Web-Formular ein. Die Referenznummer können Sie der E-Mail entnehmen.

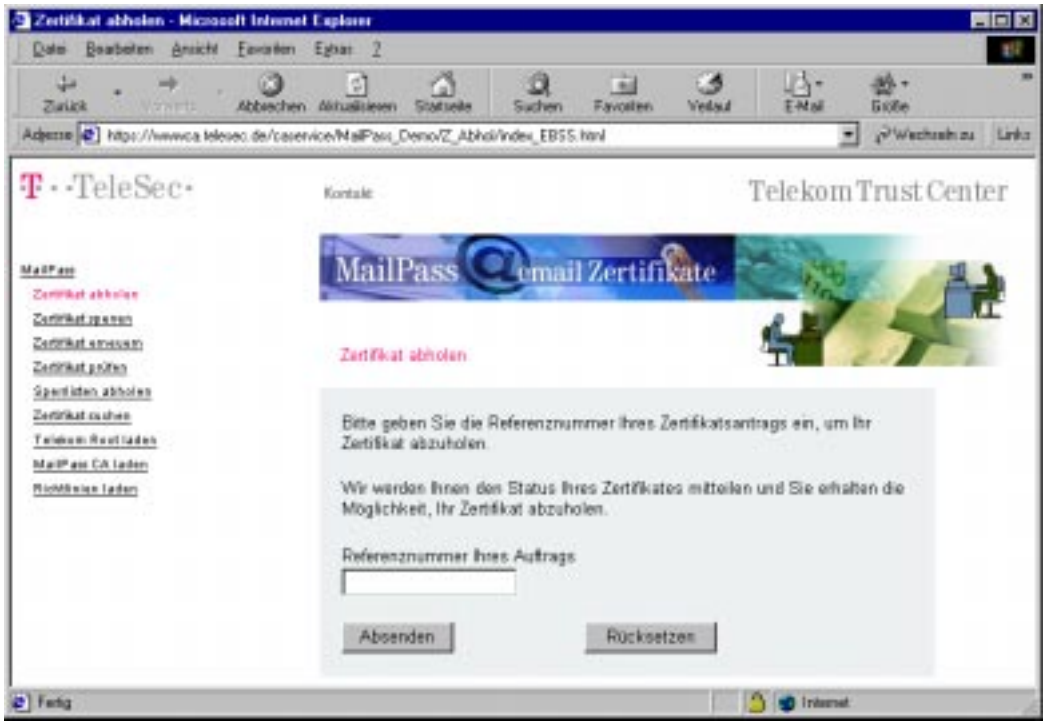
Zertifikat abholen - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Größe
Adresse https://www.ca.telesec.de/caservice/MailPass_Demo/Z_Abholindex_EBSS.html
Wechseln zu Links
T · · TeleSec ·
Kontakt
Telekom Trust Center
MailPass
Zertifikate
Zertifikat abholen
Bitte geben Sie die Referenznummer Ihres Zertifikatsantrags ein, um Ihr Zertifikat abzuholen.
Wir werden Ihnen den Status Ihres Zertifikates mitteilen und Sie erhalten die Möglichkeit, Ihr Zertifikat abzuholen.
Referenznummer Ihres Auftrags
Absenden
Rücksetzen
Fertig
Internet

Abbildung 16: Tragen Sie die Referenznummer Ihres Zertifikatantrags ein

b) Nach Klicken auf den *Absenden*-Button wird Ihr Zertifikat angezeigt.
c) Stecken Sie Ihre Smartcard in den Smartcard-Leser ein.
d) Klicken Sie auf den Button *Zertifikat abholen*.

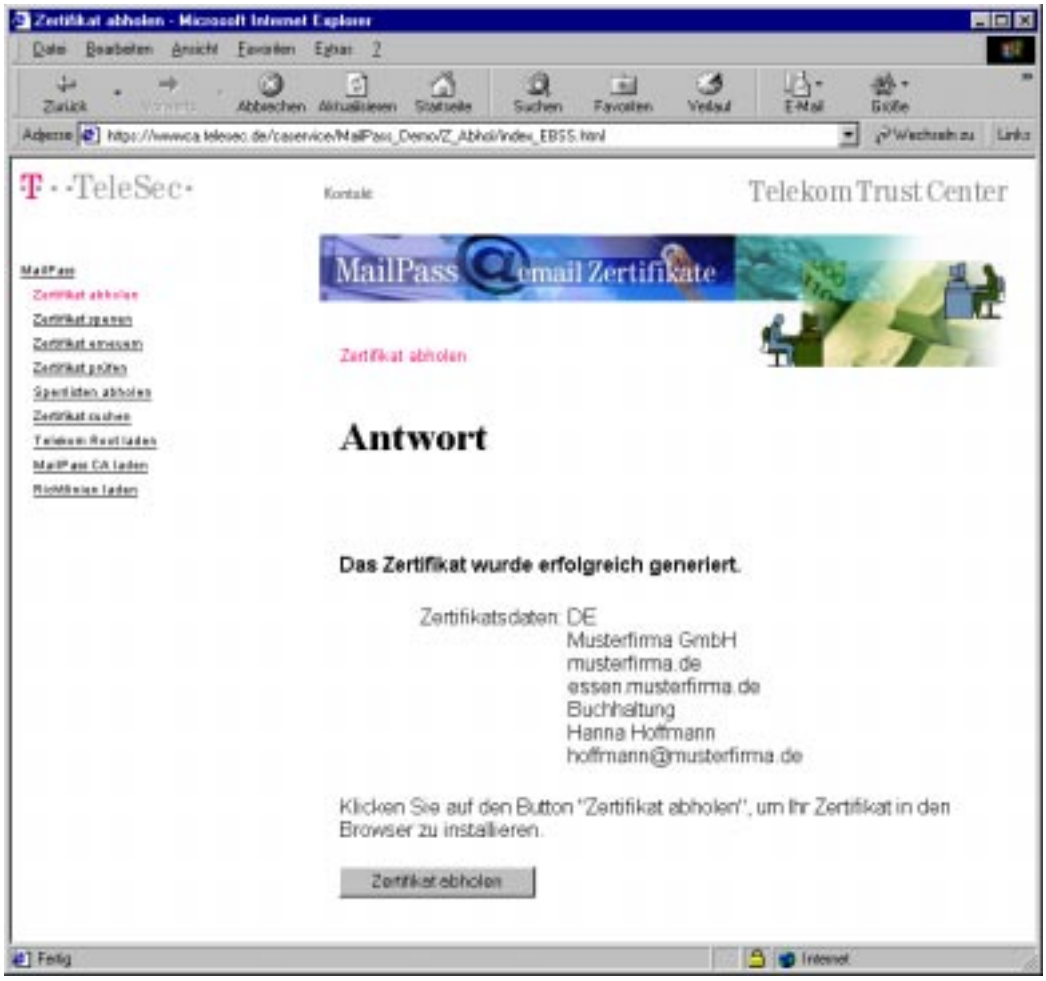

Abbildung 17: Abholen des Zertifikats

Damit wird Ihr Zertifikat auf die Smartcard geschrieben.

7) Ihre personalisierte Smartcard können Sie nun für Ihre Client-Anwendung verwenden.

Beim Einsatz von **Dual Key** ist der Ablauf nahezu identisch. Der einzige Unterschied besteht beim Laden des Zertifikats auf die Smartcard. Hier müssen beide Zertifikate separat durch Klicken der entsprechenden Buttons abgeholt werden.

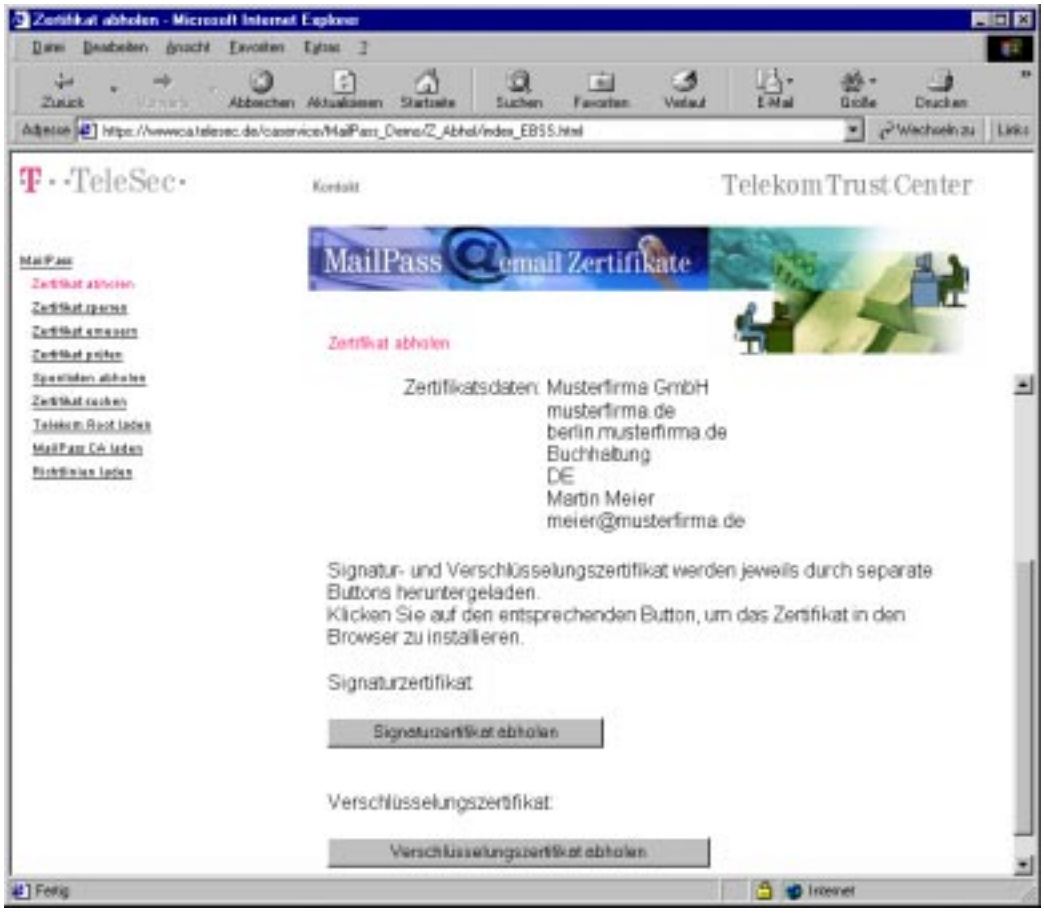

Abbildung 18: Laden der Zertifikate bei Dual Key

5.1.4 Dezentrale Registrierung über die Web-Schnittstelle beim Einsatz von Software-PSEs

Hinweis: *Wenn Sie die Beantragung mit dem Netscape Navigator durchführen, müssen Sie zunächst sicherstellen, dass die Communicator-Datenbank mit einem Passwort geschützt ist.*

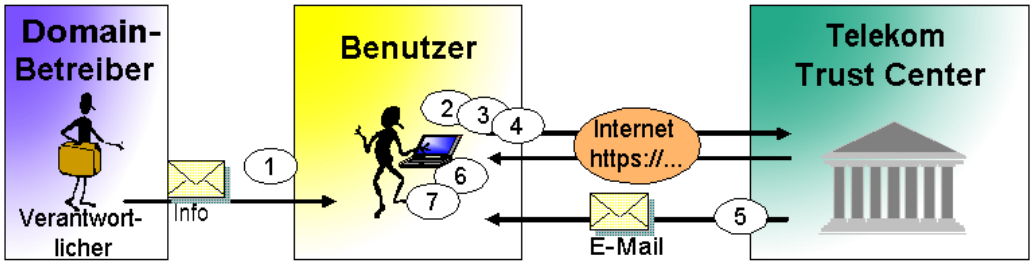

Abbildung 19: Beantragung eines Benutzerzertifikats über die Web-Schnittstelle mit Software-PSE bei dezentraler Registrierung

Abbildung 19 verdeutlicht den Ablauf der Beantragung Ihres Zertifikats. Es müssen folgende Schritte ausgeführt werden:

1) Sie werden vom MailPass-Verantwortlichen benachrichtigt, dass Sie ein Zertifikat beantragen können. Dabei wird Ihnen ein Informationsblatt übermittelt. Dieses enthält:
   - die Web-Adresse der Benutzer-Web-Schnittstelle über die Sie Ihr Zertifikat beantragen, sperren und erneuern können sowie einen dazugehörigen Benutzernamen und ein Passwort,
   - die E-Mail-Adresse und ggf. die Telefonnummer des Sub-Registrators, über den Sie die Sperrung Ihres Zertifikats veranlassen können,
   - die Nummer der Sperr-Hotline, über die Sie die Sperrung Ihres Zertifikats veranlassen können und
   - Vorgaben zum Ausfüllen des Zertifikatsantrags.
2) Sie rufen mit Ihrem Browser die Web-Seite der Benutzer-Web-Schnittstelle auf. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Diese Daten können Sie dem Informationsblatt entnehmen, welches Ihnen der MailPass-Verantwortliche übergeben hat.

Abbildung 20: Anmeldung mit Benutzername und zugehörigem Passwort

3) Wählen Sie die Funktion *Zertifikat beantragen*. Nun müssen Sie zunächst den Zuständigkeitsbereich auswählen, der Ihnen mitgeteilt wurde.

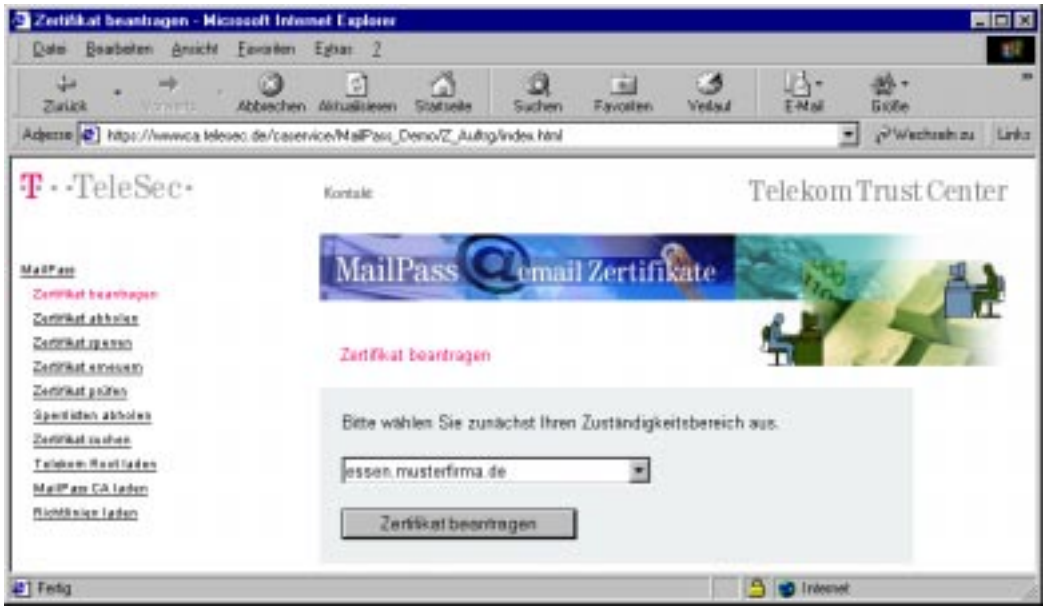

Abbildung 21: Auswählen des Zuständigkeitsbereichs

4) Nach Auswahl des Zuständigkeitsbereichs erscheint ein Online-Formular.

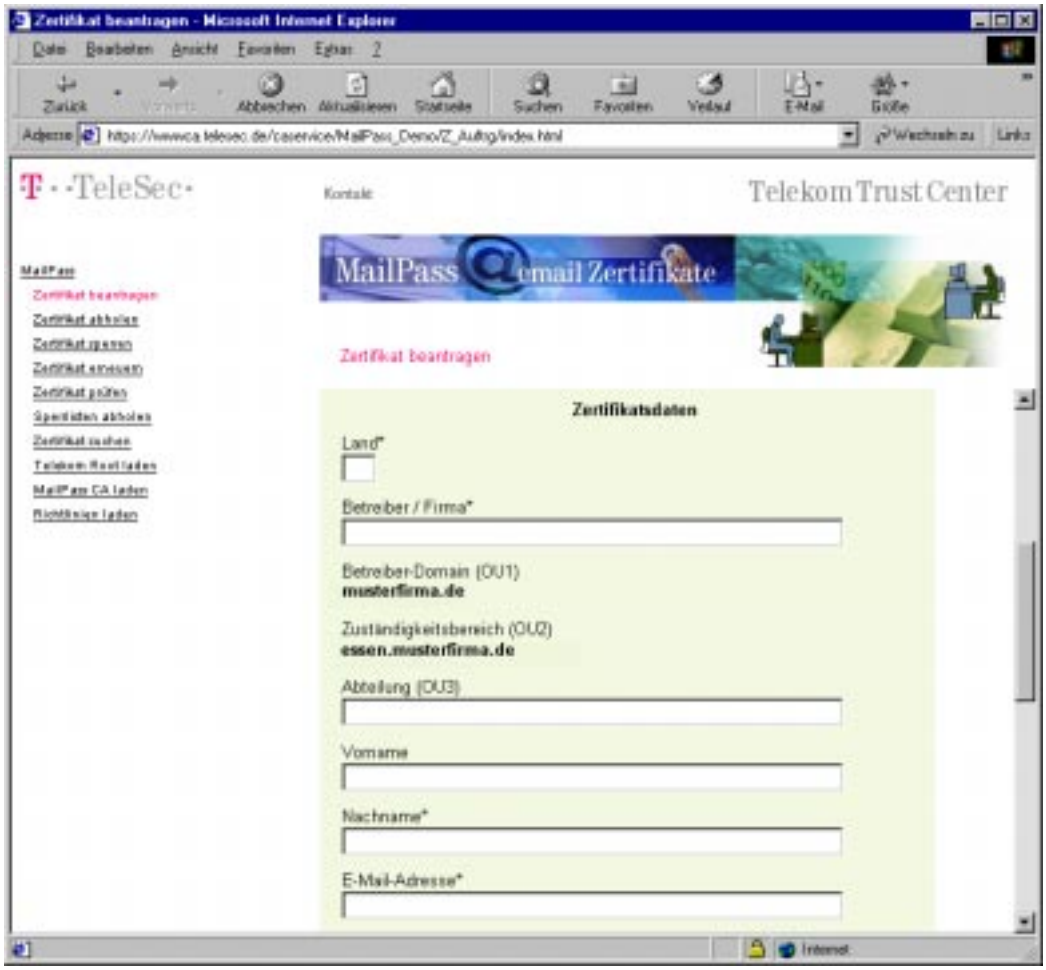

Abbildung 22: Antrag für Benutzerzertifikat

Gehen Sie bitte wie folgt vor:

a) Füllen Sie die Datenfelder aus. Beachten Sie dabei bitte die Vorgaben ihres MailPass-Verantwortlichen. Beachten Sie des Weiteren, dass Vor- und Nachname keine Umlaute enthalten dürfen. Gültige Zeichen sind: *a-z A-Z 0-9 ' ( ) + , . / : ? = -*

b) Tragen Sie die Authentifizierungsdaten ein. Von besonderer Wichtigkeit ist das Sperrpasswort. Dieses müssen Sie sich gut merken, da es abgefragt wird, wenn Sie Ihr Zertifikat sperren lassen.

c) Für das Feld zur Auswahl des Schlüsselgenerators wählen Sie bitte folgende Einstellungen:
   - Netscape Navigator: *1024 (Verschlüsselung hoher Komplexität)*

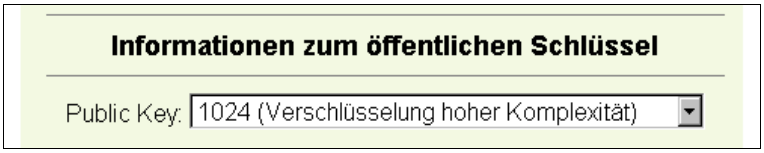

Abbildung 23: Einstellen der Schlüssellänge (Netscape)

   - MS Internet Explorer: *Microsoft Enhanced Cryptographic Provider*

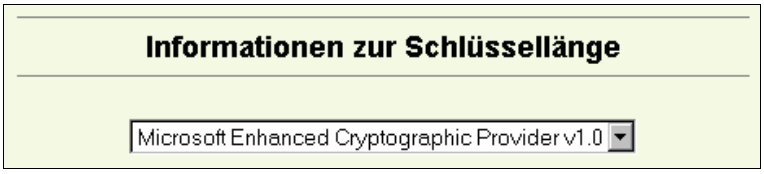

Abbildung 24: Einstellen der Schlüssellänge (Internet Explorer)

d) Klicken Sie auf den Button *Absenden*.
Wenn Sie den Netscape Navigator verwenden, erscheint ein neues Fenster, in dem Sie die Erzeugung Ihres privaten Schlüssels mit *OK* bestätigen müssen.

Private Key erstellen - Netscape
Private Key erstellen
Klicken Sie auf "OK". Für Ihr Zertifikat wird nun ein Private Key erstellt
Dies kann einige Minuten dauern.
Wichtig: Wird dieser Vorgang unterbrochen, müssen Sie das Zertifikat erneut anfordern.
Mehr Info...
OK
Abbrechen

Abbildung 25: Start der Schlüsselgenerierung

Sie müssen anschließend das Passwort für die Sicherheitsumgebung Ihres Browsers angeben. Falls diese noch nicht durch ein Passwort geschützt ist, werden Sie aufgefordert ein Passwort zu setzen. Da sich Ihr privater Schlüssel in dieser Sicherheitsumgebung befindet, sollten Sie ein starkes Passwort wählen (beachten Sie hierbei bitte die Hinweise im Kapitel 6.2).

e) Auf der Antwortseite in Ihrem Browser wird die Referenznummer Ihres Zertifikatsantrags angezeigt.

5) Nach der Erzeugung Ihres Zertifikats im Telekom Trust Center werden Sie per E-Mail benachrichtigt. Die E-Mail enthält die Referenznummer Ihres Antrags und die Web-Adresse, über die Sie Ihr Zertifikat abholen können.
6) Sie rufen mit Ihrem Browser die in der E-Mail angegebene Web-Seite auf. Alternativ können Sie auch über die Benutzer-Web-Schnittstelle die Funktion *Zertifikat abholen* aufrufen.
   a) Tragen Sie die Referenznummer Ihres Zertifikatsantrags in das vorgesehene Web-Formular ein. Die Referenznummer können Sie der E-Mail entnehmen.

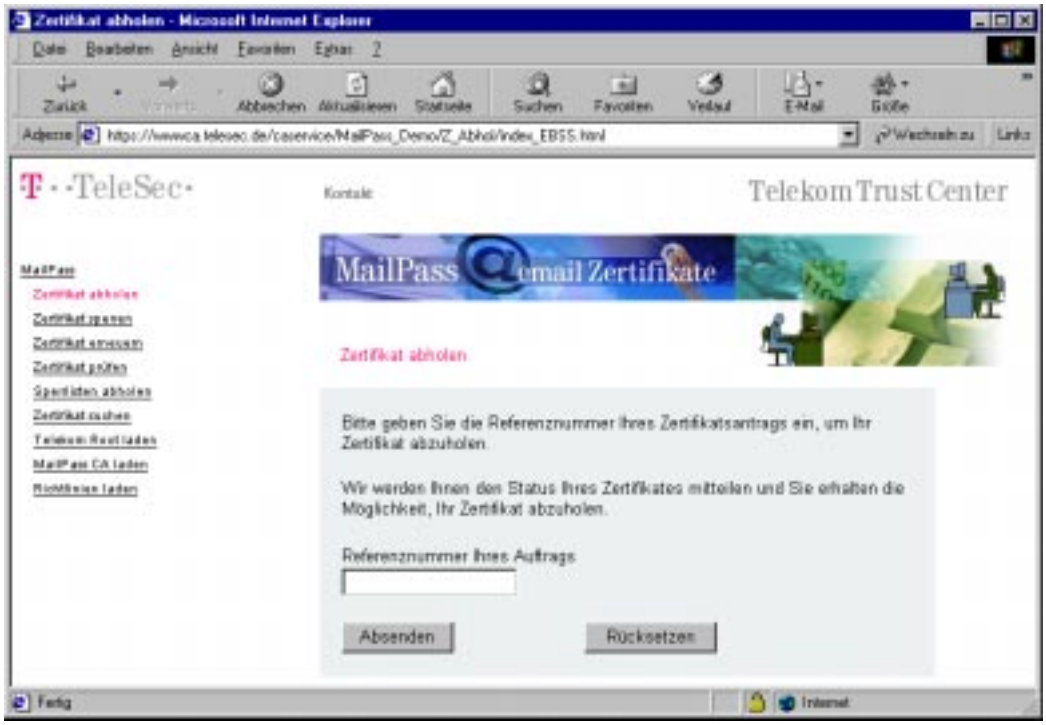
Zertifikat abholen - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Größe
Adresse https://www.ca.telesec.de/caservice/MailPass_Demo/Z_Abholindex_EBSS.html
Wechseln zu Links
T · · TeleSec ·
Kontakt
Telekom Trust Center
MailPass
Zertifikate
Zertifikat abholen
Bitte geben Sie die Referenznummer Ihres Zertifikatsantrags ein, um Ihr Zertifikat abzuholen.
Wir werden Ihnen den Status Ihres Zertifikates mitteilen und Sie erhalten die Möglichkeit, Ihr Zertifikat abzuholen.
Referenznummer Ihres Auftrags
Absenden
Rücksetzen
Fertig
Internet

Abbildung 26: Tragen Sie die Referenznummer Ihres Zertifikatantrags ein

b) Nach Klicken auf den *Absenden*-Button wird Ihr Zertifikat angezeigt.
c) Klicken Sie auf den Button *Zertifikat abholen*.

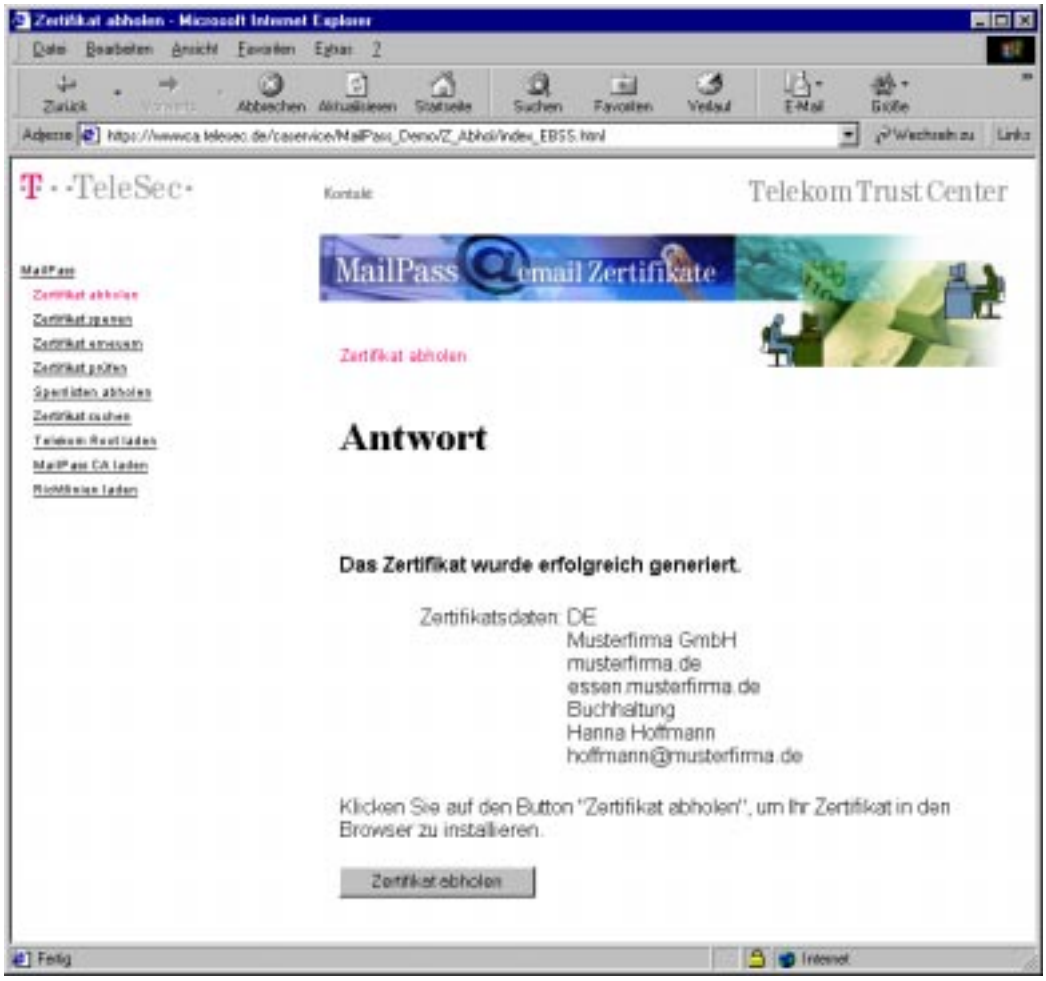

Abbildung 27: Zertifikat im Browser speichern

Damit wird Ihr Zertifikat in Ihrem Browser gespeichert.

Beim Einsatz von **Dual Key** ist der Ablauf nahezu identisch. Der einzige Unterschied besteht beim Laden des Zertifikats in die Browser-Datenbank. Hier müssen beide Zertifikate separat durch Klicken der entsprechenden Buttons abgeholt werden.

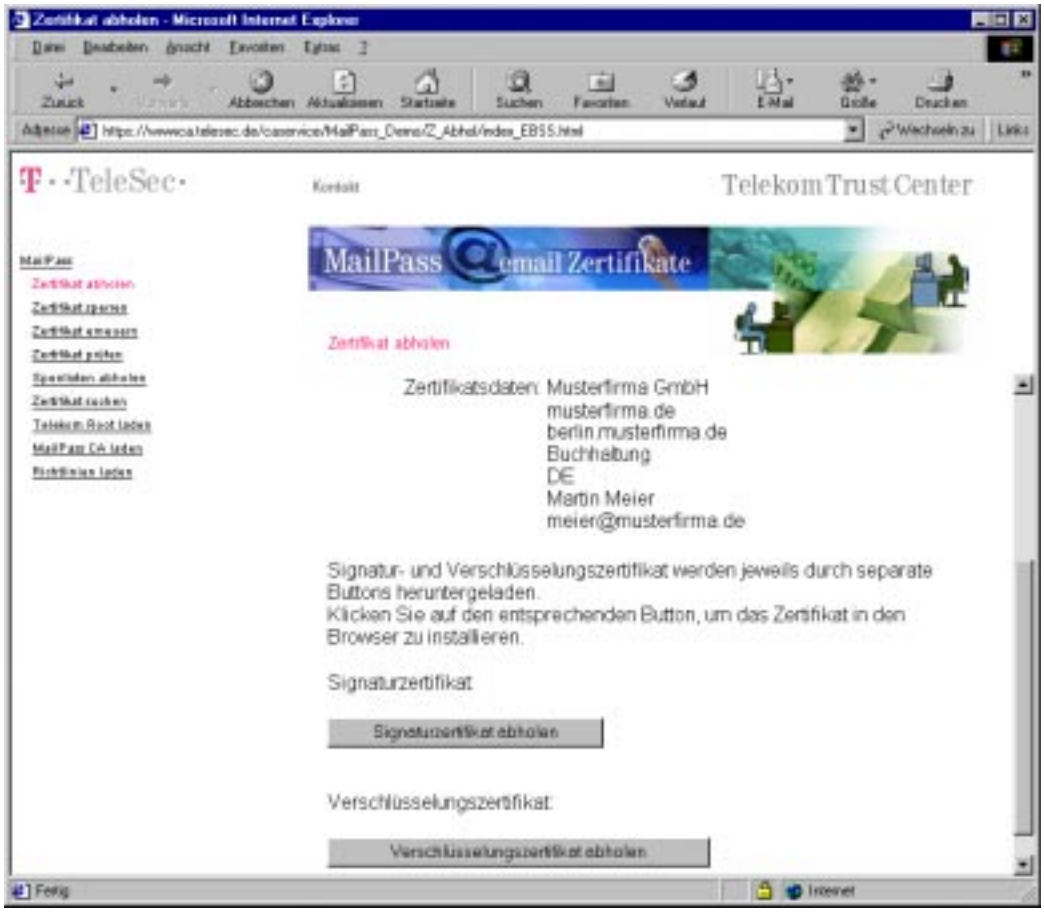

Abbildung 28: Laden der Zertifikate bei Dual Key

Wenn Sie Ihr Zertifikat mit dem Internet Explorer beantragt und geladen haben, können Sie es nun mit Microsoft Outlook verwenden. Wenn Sie Ihr Zertifikat mit dem Netscape Navigator beantragt und geladen haben, können Sie es mit dem Netscape Messanger verwenden. Für den Fall, dass Sie nicht den zum E-Mail-Programm korrespondierenden Browser verwendet haben oder Ihr Zertifikat mit einer anderen Anwendungssoftware nutzen möchten, müssen Sie Ihren privaten Schlüssel und das Zertifikat noch in eine PKCS#12-Datei exportieren. Dieser Ablauf ist in Kapitel 5.5 beschrieben.

5.1.5 Dezentrale Registrierung über die Mail-Request-Schnittstelle

Die Mail-Request-Schnittstelle erlaubt Ihnen die dezentrale Registrierung per E-Mail. Zu diesem Zweck müssen Sie zunächst mit einer geeigneten Client-Anwendung einen Zertifikatsantrag im Format PKCS#10 erzeugen. Diesen schicken Sie dann per E-Mail an das Telekom Trust Center. Die E-Mail-Adresse erfahren Sie von Ihrem MailPass-Verantwortlichen. Anschließend nehmen Sie Kontakt mit Ihrem Sub-Registrator auf und handeln ein Sperrpasswort aus. Bei erfolgreicher Bearbeitung Ihres Antrags wird Ihnen dann das Zertifikat direkt per E-Mail zugeschickt.
Nähere Informationen zum Erzeugen des Zertifikatsantrags im Format PKCS#10 bzw. zum Import des erhaltenen Zertifikats in Ihre Client-Anwendung entnehmen Sie bitte den entsprechenden Benutzerhandbüchern Ihrer Client-Anwendung.

Für weitere Fragen bezüglich der dezentralen Registrierung über die Mail-Request-Schnittstelle wenden Sie sich bitte an Ihren MailPass-Verantwortlichen.

5.2 Sperren eines Zertifikats

In bestimmten Fällen ist es erforderlich, dass Sie Ihr Zertifikat sperren lassen. Dies ist insbesondere dann notwendig, wenn Ihr privater Schlüssel in fremde Hände gelangt ist. Im Folgenden werden alle Gründe aufgelistet, bei denen Sie die Sperrung Ihres Zertifikats veranlassen müssen:

- Ihr privater Schlüssel ist kompromittiert, das heißt eine andere Person ist in den Besitz Ihres privaten Schlüssels gekommen.
- Es besteht der Verdacht, dass Ihr privater Schlüssel kompromittiert wurde.
- Ihre Smartcard bzw. Ihr Software-PSE ist defekt und Sie können deshalb Ihren Schlüssel nicht mehr nutzen.[1]
- Sie haben die PIN für Ihre Smartcard bzw. das Passwort für Ihr Software-PSE vergessen.[2]
- Die Angaben in Ihrem Zertifikat sind nicht mehr aktuell. Dies kann zum Beispiel der Fall sein, wenn die im Zertifikat angegebene E-Mail-Adresse nicht mehr gültig ist oder wenn Sie einem neuen Zuständigkeitsbereich zugeordnet werden.

Um Ihr Zertifikat sperren zu lassen, stehen Ihnen verschiedene Möglichkeiten zur Verfügung:

- **Benutzer-Web-Schnittstelle / eingeschränkte Benutzer-Web-Schnittstelle:** Die Adresse dieser Web-Seite können Sie dem Informationsblatt entnehmen, welches Sie von Ihrem MailPass-Verantwortlichen bzw. Ihrem Sub-Registrator erhalten haben.
- **Sub-Registrator:** Sie können per E-Mail oder Telefon (ggf. auch persönlich) bei Ihrem Sub-Registrator die Sperrung Ihres Zertifikats anfordern. Die E-Mail-Adresse und die Telefonnummer können Sie ebenfalls dem Informationsblatt entnehmen. Des Weiteren sind diese Daten über die Funktion *Zertifikat sperren* der Benutzer-Web-Schnittstelle einsehbar.
- **Sperr-Hotline:** Unter der im Informationsblatt angegebenen Rufnummer können Sie telefonisch die vorläufige Sperrung Ihres Zertifikats veranlassen. Die Rufnummer kann außerdem der Benutzer-Web-Schnittstelle entnommen werden.

5.2.1 Sperren eines Zertifikats über die (eingeschränkte) Benutzer-Web-Schnittstelle

Voraussetzung des nachfolgend beschriebenen Ablauf ist die Kenntnis Ihres Sperrpassworts. Sollten Sie Ihr Sperrpasswort vergessen haben, fordern Sie bitte die Sperrung persönlich bei Ihrem Sub-Registrator an.

1) Sie rufen mit Ihrem Browser die Web-Seite der Benutzer-Web-Schnittstelle bzw. der eingeschränkten Benutzer-Web-Schnittstelle auf. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Diese Daten können Sie dem Informationsblatt entnehmen, welches Ihnen der MailPass-Verantwortliche bzw. der Sub-Registrator übergeben hat.
2) Wählen Sie die Funktion *Zertifikat sperren*.

[1] Wenn Sie ein Software-PSE verwenden und Ihr Zertifikat selbst mit Ihrem Browser geladen haben, dann befindet sich ihr privater Schlüssel und das Zertifikat noch im Browser. Sie können Ihren Schlüssel und das Zertifikat erneut aus dem Browser in eine Datei (*.p12) speichern. In diesem Fall brauchen Sie Ihr Zertifikat nicht sperren zu lassen.
[2] Wie 1

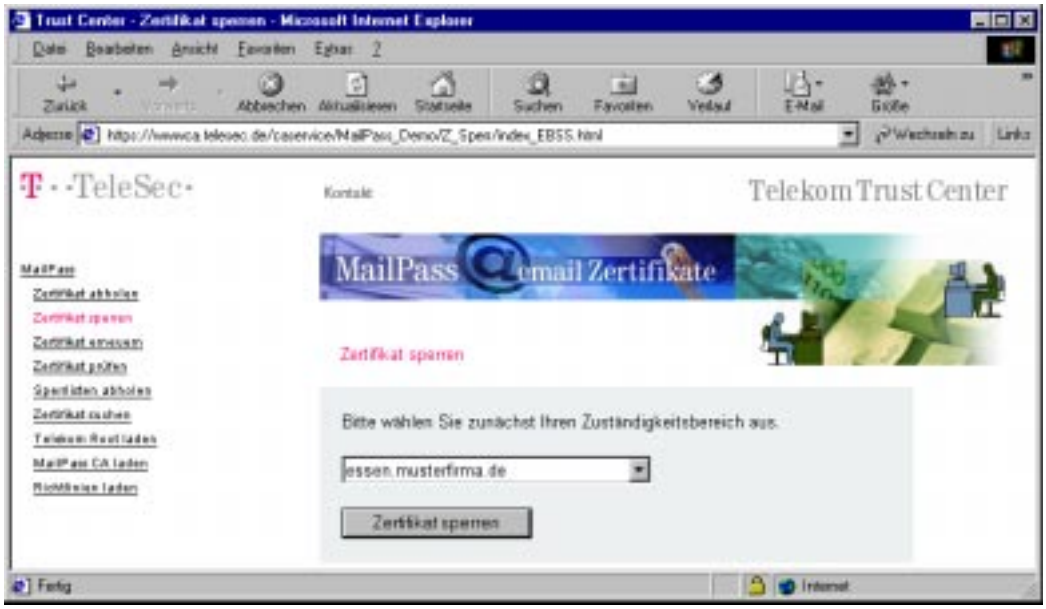

Abbildung 29: Auswahl des Zuständigkeitsbereichs

3) Wählen Sie Ihren Zuständigkeitsbereich aus der Auswahlliste.

Trust Center - Zertifikat sperren - Microsoft Internet Explorer
TeleSec
Kontakt
Telekom Trust Center
MailPass email Zertifikate
Zertifikat sperren
Ihr Zertifikat kann gesperrt werden, wenn Sie befürchten, dass Ihr geheimer Schlüssel ausspioniert wurde und von unberechtigten Personen genutzt werden könnte. Durch das Sperren wird ein Zertifikat auf die so genannte Sperrliste gesetzt. Diese enthält die Seriennummern von Zertifikaten, die vor Ablauf ihrer regulären Gültigkeit für ungültig erklärt wurden.
Sie haben die Möglichkeit, Zertifikate nach den nebenstehenden Kriterien zu sperren. Über die Sperrung Ihres Zertifikats werden Sie dann per E-Mail informiert.
Referenznummer
Seriennummer
E-Mail-Adresse

Abbildung 30: Zertifikat sperren

4) Sie haben verschiedene Kriterien zur Auswahl, über die Sie Ihr zu sperrendes Zertifikat angeben können:
   - *Referenznummer*: Hier müssen Sie die Referenznummer Ihres Zertifikatsantrags und Ihr Sperrpasswort eingeben.

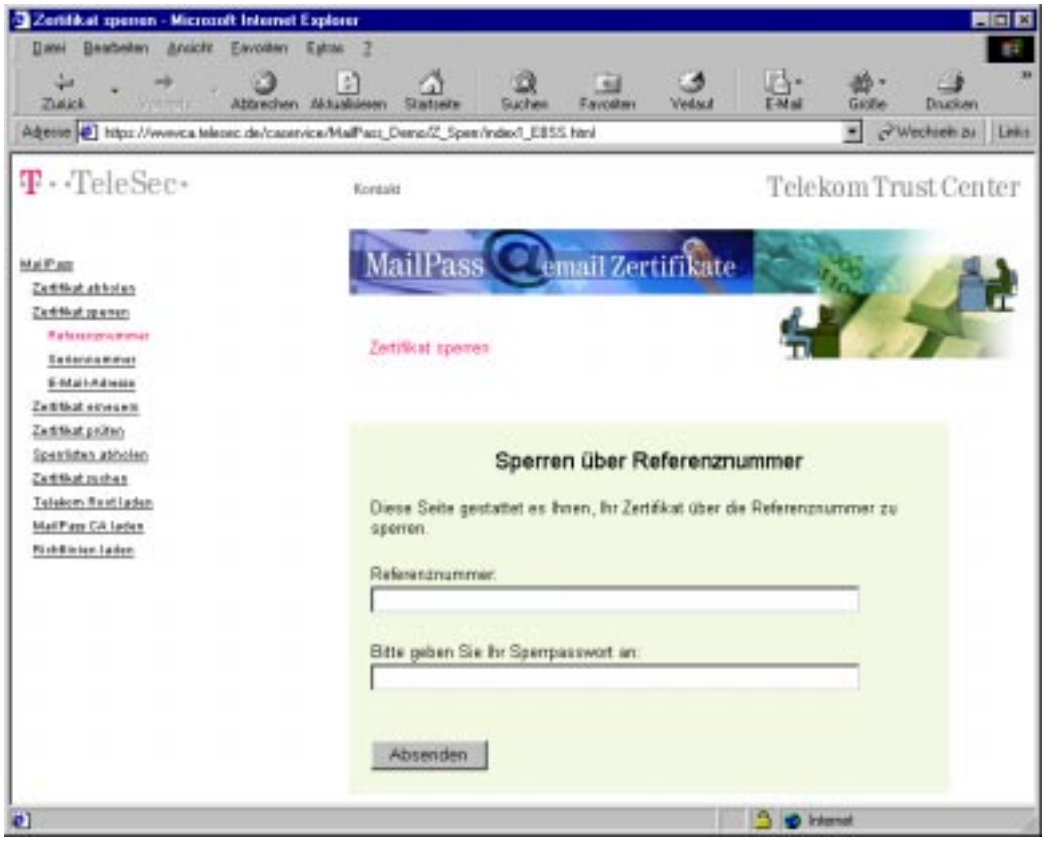

Abbildung 31: Sperren über Angabe der Referenznummer

- *Seriennummer*: Hier müssen Sie die Seriennummer Ihres Zertifikats und Ihr Sperrpasswort eingeben.

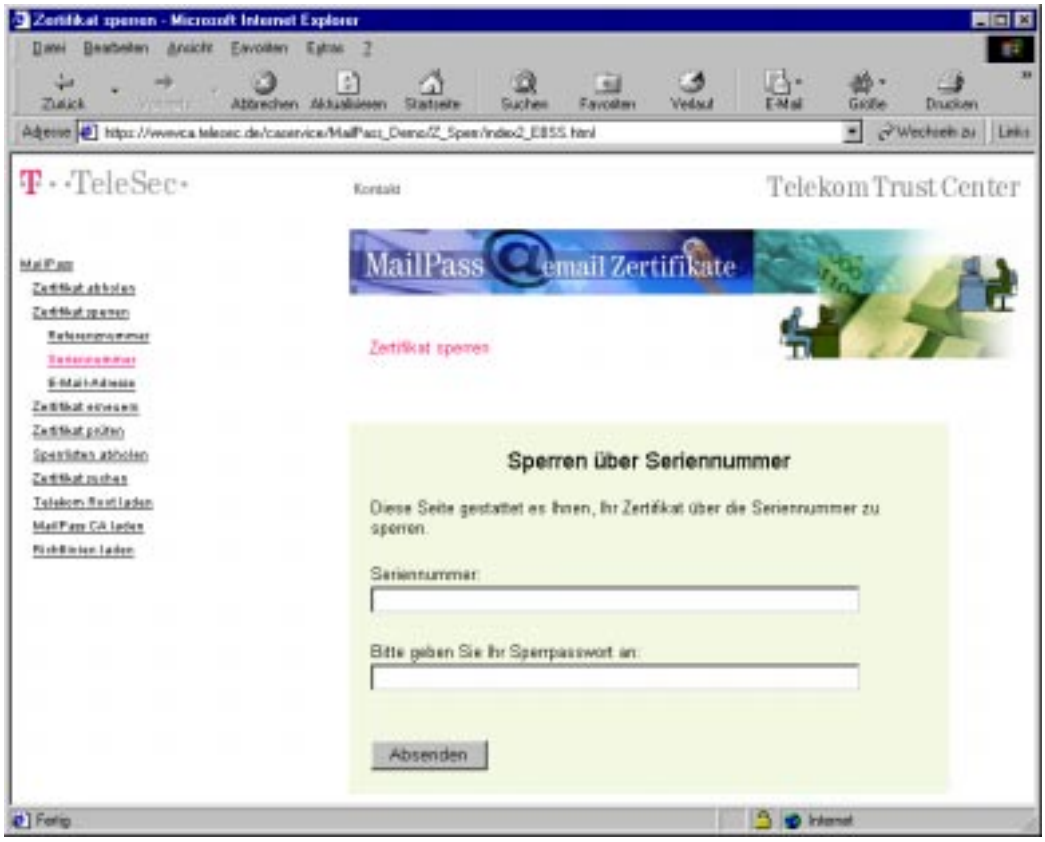

Abbildung 32: Sperren über Angabe der Seriennummer

- *E-Mail-Adresse*:
  - Hier müssen Sie die im Zertifikat angegebene E-Mail-Adresse und Ihr Sperrpasswort eintragen.

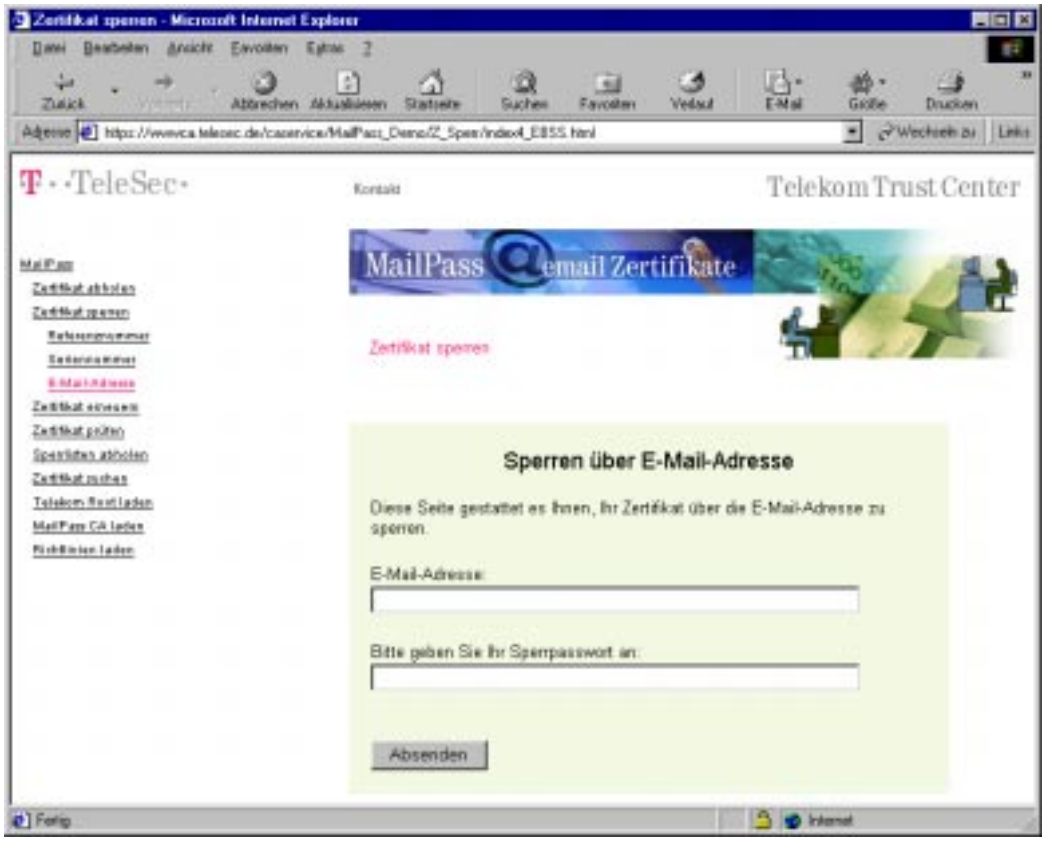

Abbildung 33: Sperren über Angabe der E-Mail-Adresse

- Wählen Sie das zu sperrende Zertifikat aus der Liste.

Abbildung 34: Auswahl des zu sperrenden Zertifikats

- Es erfolgt eine automatische Weiterleitung zur Funktion Sperren über Seriennummer. Dabei müssen Sie nochmals das Sperrpasswort eingeben.

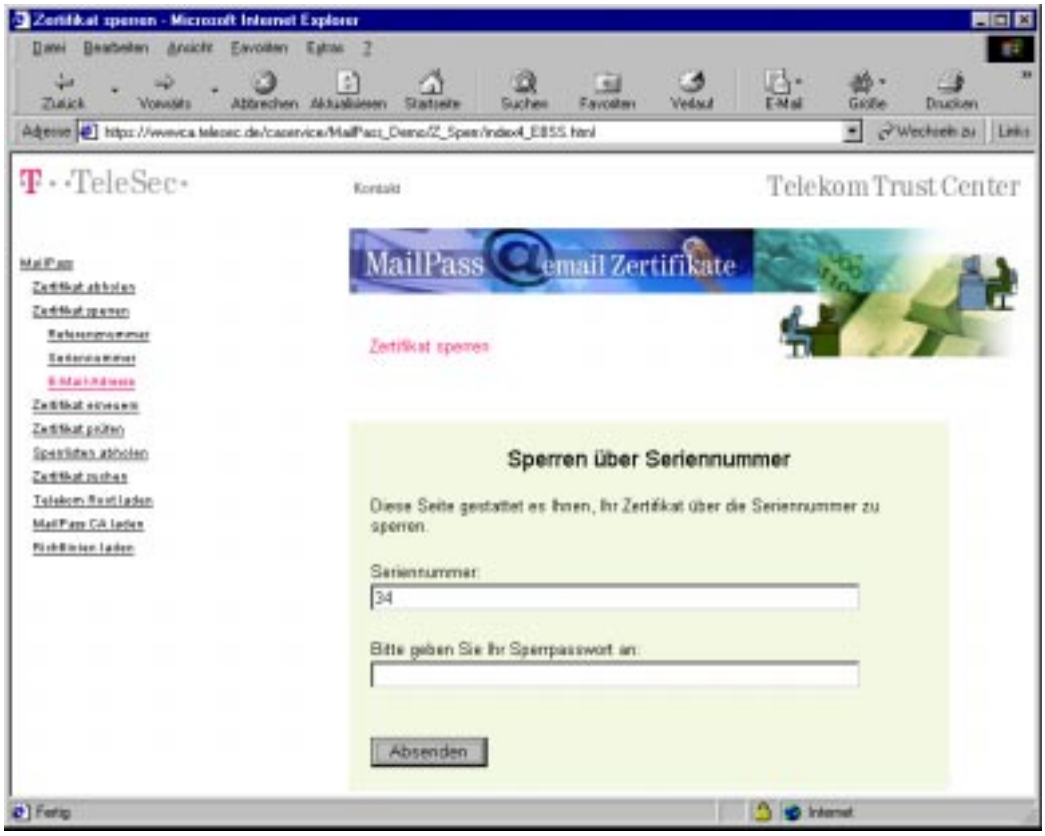

Abbildung 35: Erneute Eingabe des Sperrpassworts

5) Wenn Ihr Sperrpasswort korrekt ist, wird Ihnen Ihr Zertifikat angezeigt.

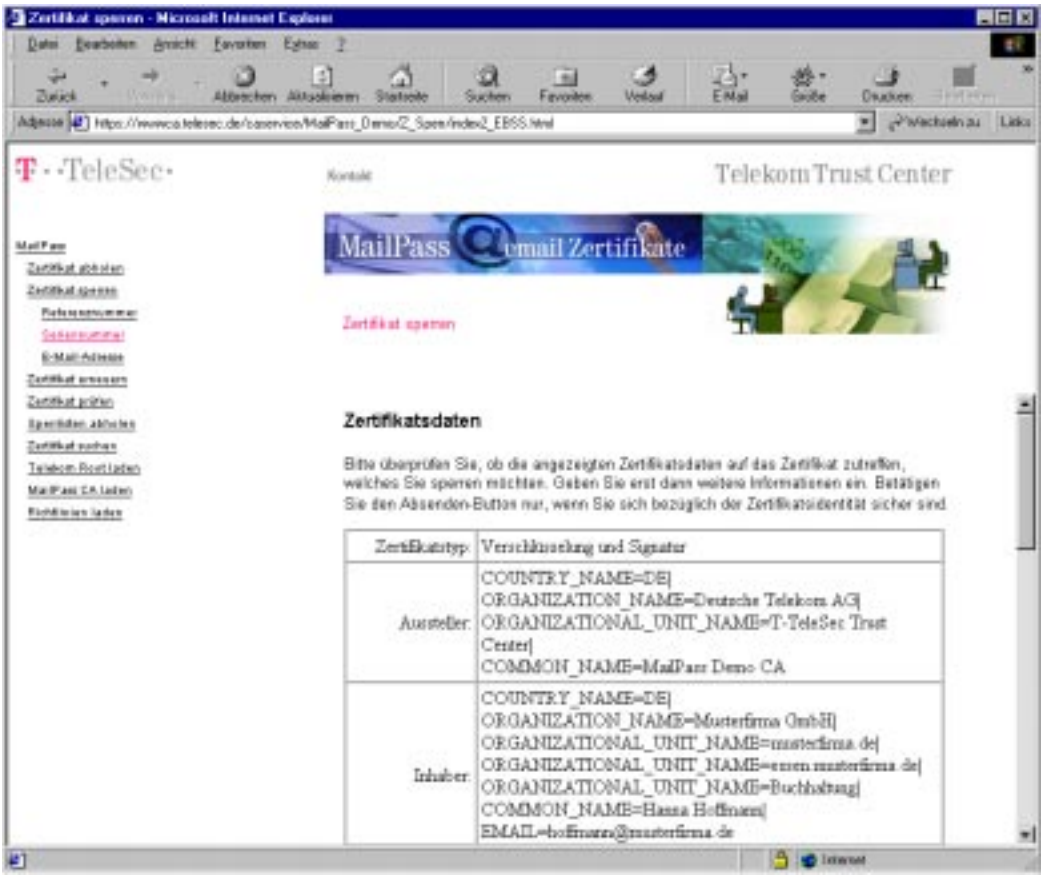
Zertifikat sperren - Microsoft Internet Explorer
TeleSec
Telekom Trust Center
MailPass email Zertifikate
Zertifikat sperren
Zertifikatsdaten
Bitte überprüfen Sie, ob die angezeigten Zertifikatsdaten auf das Zertifikat zutreffen, welches Sie sperren möchten. Geben Sie erst dann weitere Informationen ein. Bestätigen Sie den Absenden-Button nur, wenn Sie sich bezüglich der Zertifikatsidentität sicher sind.
Zertifikatstyp: Verschlüsselung und Signatur
Aussteller: COUNTRY_NAME=DE| ORGANIZATION_NAME=Deutsche Telekom AG| ORGANIZATIONAL_UNIT_NAME=T-TeleSec Trust Center| COMMON_NAME=MailPass Demo CA
Inhaber: COUNTRY_NAME=DE| ORGANIZATION_NAME=Musterfirma GmbH| ORGANIZATIONAL_UNIT_NAME=musterfirma.de| ORGANIZATIONAL_UNIT_NAME=einen.musterfirma.de| ORGANIZATIONAL_UNIT_NAME=Buchhaltung| COMMON_NAME=Hanna Hoffmann| EMAIL=hoffmann@musterfirma.de

Abbildung 36: Formular zum Sperren eines Zertifikats – Zertifikatsdaten

a) Überprüfen Sie, ob es sich bei dem angezeigten Zertifikat um das zu sperrende Zertifikat handelt.
b) Tragen Sie im dafür vorgesehenen Feld den Zeitpunkt ein, ab dem Ihr Zertifikat als ungültig erklärt werden soll.
c) Wählen Sie einen Grund der Sperrung aus.
d) Klicken Sie auf den Button *Absenden*.

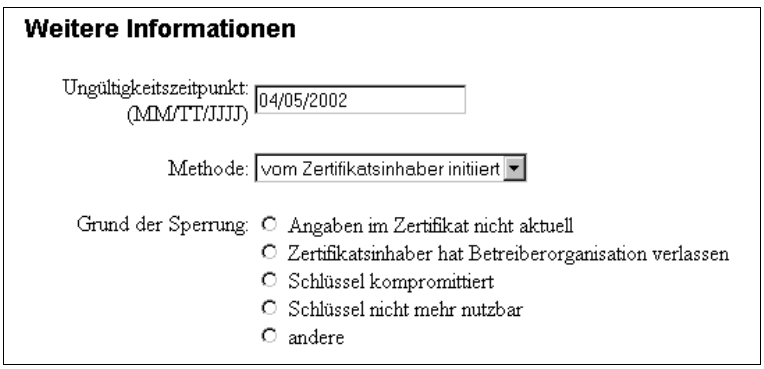

Abbildung 37: Formular zum Sperren eines Zertifikats – Zeitpunkt und Sperrgrund

6) Ihr Zertifikat ist nun gesperrt und kann nicht mehr verwendet werden. Die Sperrung wird per E-Mail vom Telekom Trust Center bestätigt.

5.2.2 Sperren eines Zertifikats über den Sub-Registrator

Bei der Registrierung haben Sie die E-Mail-Adresse und ggf. auch die Telefonnummer eines verantwortlichen Sub-Registrators erhalten. Zum Sperren Ihres Zertifikats können Sie an diese Adresse eine E-Mail mit folgendem Inhalt senden:

- Referenznummer Ihres Zertifikatsantrages, Seriennummer Ihres Zertifikats oder die E-Mail-Adresse, die in Ihrem Zertifikat enthalten ist
- Ihren Namen und die Abteilung
- Grund für die Sperrung Ihres Zertifikats
- Sperrpasswort

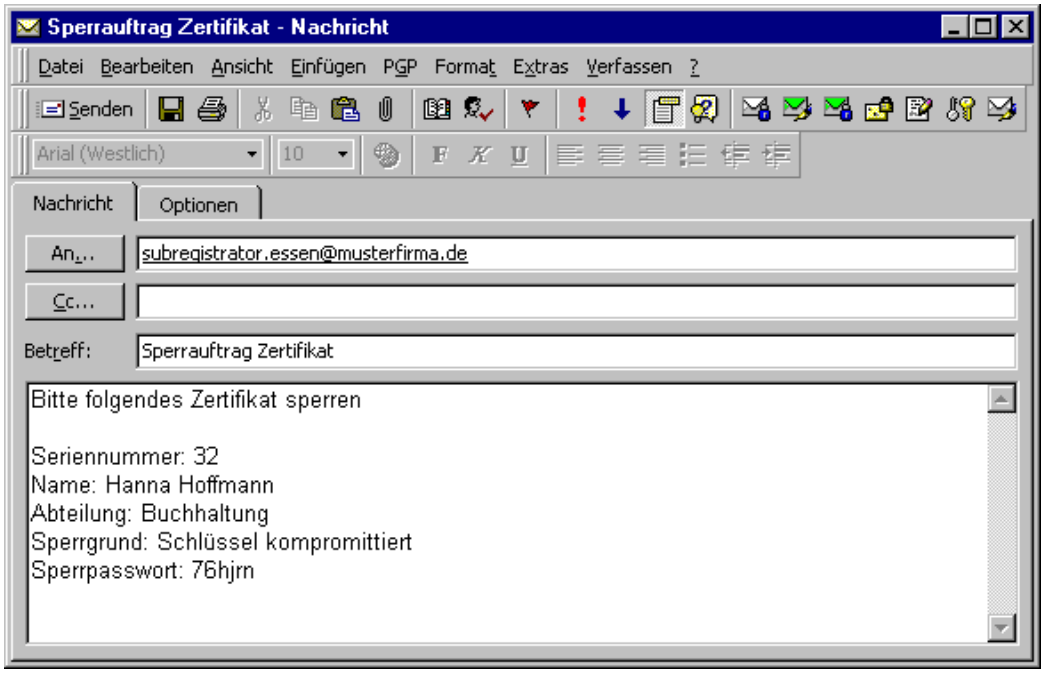

Abbildung 38: Beispiel für eine E-Mail zum Sperren des Benutzerzertifikats

Der Sub-Registrator prüft anhand des angegebenen Sperrpassworts, ob Sie berechtigt sind, das Zertifikat zu sperren. Danach veranlasst der Sub-Registrator die Sperrung Ihres Zertifikats. Die Sperrung ist endgültig. Sie werden per E-Mail vom Trust Center über die Sperrung informiert.

Sollten Sie Ihr Sperrpasswort nicht mehr zur Verfügung haben, müssen Sie persönlich bei Ihrem Sub-Registrator erscheinen. Dieser prüft dann Ihre Identität anhand eines Ausweisdokumentes und veranlasst die Sperrung Ihres Zertifikats.

5.2.3 Sperren eines Zertifikats über die Sperr-Hotline

Bei der Registrierung haben Sie die Telefonnummer einer Sperr-Hotline erhalten. Diese Telefonnummer können Sie außerdem über die Funktion *Zertifikat sperren* der Benutzer-Web-Schnittstelle erhalten. Zum Sperren Ihres Zertifikats können Sie dort anrufen. Folgende Angaben werden zwingend benötigt:

- Ihr Name
- Name des Telekom-Services, hier also T-TeleSec MailPass
- Name Ihres Domain-Betreibers
- Art des zu sperrenden Zertifikats, in diesem Fall Benutzerzertifikat

- Referenznummer Ihres Zertifikatsantrages, Seriennummer Ihres Zertifikats oder die E-Mail-Adresse aus Ihrem Zertifikat
- Grund für die Sperrung Ihres Zertifikats
- Rufnummer, unter welcher Sie für Rückfragen zur Verfügung stehen

Das Hotline-Personal nimmt Ihren Sperrantrag entgegen. Wenn die von Ihnen angegebenen Daten auf ein Zertifikat zutreffen, wird eine vorläufige Sperrung Ihres Zertifikats veranlasst.
Eventuell erfolgt noch ein Rückruf durch einen Sperr-Hotline-Operator, um unkorrekte Angaben berichtigen zu können.

Um das Zertifikat endgültig sperren zu lassen, müssen Sie sich an Ihren Sub-Registrator wenden. Befolgen Sie dafür bitte den in Kapitel 5.2.2 beschriebenen Ablauf.

5.3 Erneuern eines Zertifikats

Ihr Zertifikat hat eine begrenzte Gültigkeitsdauer. Vor Ablauf dieser Zeit werden Sie per E-Mail daran erinnert, Ihr Zertifikat zu erneuern. Hierfür steht Ihnen die Benutzer-Web-Schnittstelle bzw. die eingeschränkte Benutzer-Web-Schnittstelle zur Verfügung.

Die Prozesse der Erneuerung eines Zertifikats bei Verwendung von Smartcards und Verwendung von Software-PSEs unterscheiden sich. Sie brauchen nur das für Sie relevante Kapitel betrachten.

5.3.1 Einsatz von Smartcards

Dieser Ablauf kann nur durchgeführt werden, wenn Ihr zu erneuerndes Zertifikat gültig ist und mit dem zugehörigen privaten Schlüssel auf einer Smartcard vorliegt.

Wenn Sie als Browser den Internet Explorer einsetzen, dann müssen Sie Ihr Zertifikat, welches sich auf der Smartcard befindet, zunächst dem Browser bekannt machen. Falls dies noch nicht geschehen ist, befolgen Sie bitte den Ablauf in Kapitel 5.5.

Um Ihr Zertifikat zu erneuern gehen Sie wie folgt vor:

1) Sie erhalten vom Telekom Trust Center eine E-Mail, in der Sie über den Ablauf Ihres Zertifikats informiert werden.
2) Rufen Sie mit Ihrem Browser die Web-Seite der Benutzer-Web-Schnittstelle bzw. der eingeschränkten Benutzer-Web-Schnittstelle auf. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Diese Daten können Sie dem Informationsblatt entnehmen, welches Sie bei der Registrierung erhalten haben.

Abbildung 39: Geben Sie Benutzernamen und Passwort für die Benutzer-Web-Schnittstelle ein

3) Stecken Sie Ihre Smartcard in den Smartcard-Leser ein.
4) Wählen Sie die Funktion *Zertifikat erneuern*. Bei Einsatz des Netscape Navigators wird nun Ihre PIN abgefragt. Damit nur Sie in der Lage sind, Ihr Zertifikat zu erneuern, wird eine SSL-Client-Authentifizierung durchgeführt. Hierfür müssen Sie das Zertifikat angeben, welches Sie erneuern möchten. Wählen Sie dafür die Smartcard aus. Bei Einsatz des MS Internet Explorers müssen Sie nun Ihre PIN eingeben.

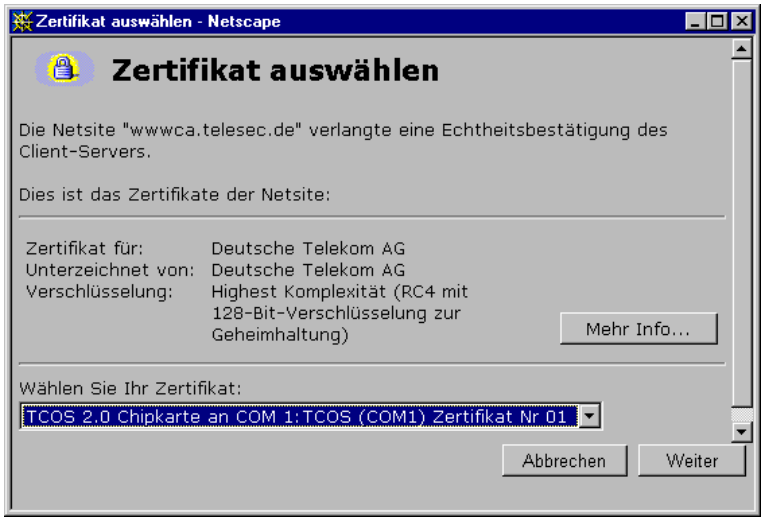

Abbildung 40: Wählen Sie das zu erneuernde Zertifikat aus (Netscape)

Clientauthentifizierung
Identifikation
Die Website, die Sie sich anzeigen lassen möchten, fordert eine Identifikation. Wählen Sie das Zertifikat aus, das für die Verbindung verwendet werden soll.
Hanna Hoffmann
Details...
Zertifikat anzeigen...
OK
Abbrechen

Abbildung 41: Wählen Sie das zu erneuernde Zertifikat aus (Internet Explorer)

5) Es erscheint ein Online-Formular, auf dem Ihnen Ihr Zertifikat angezeigt wird.

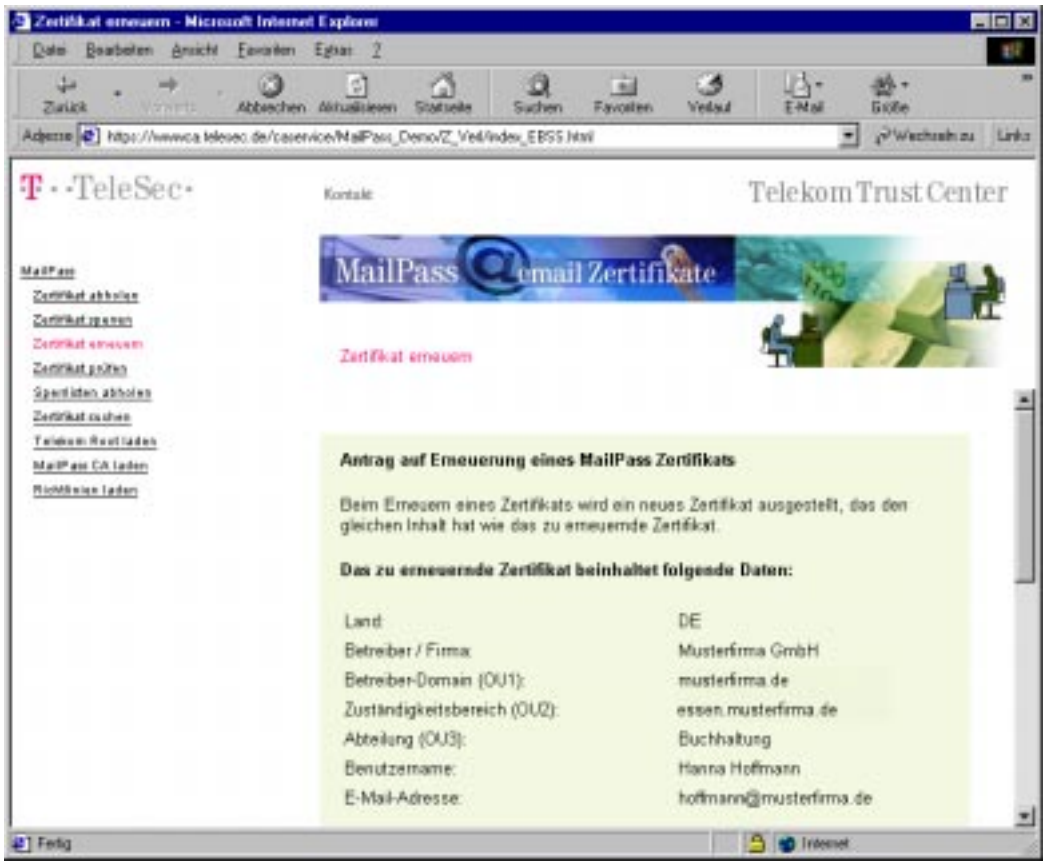

Abbildung 42: Antrag auf Erneuerung eines Benutzerzertifikats

Gehen Sie bitte wie folgt vor:

a) Für das Feld zur Auswahl des Schlüsselgenerators wählen Sie bitte folgende Einstellungen:
   - Netscape Navigator: *1024 (Verschlüsselung hoher Komplexität)*

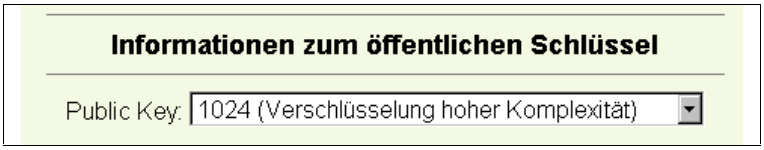

Abbildung 43: Einstellen der Schlüssellänge (Netscape)

   - MS Internet Explorer: *Kobil Smart CSP v1.0*

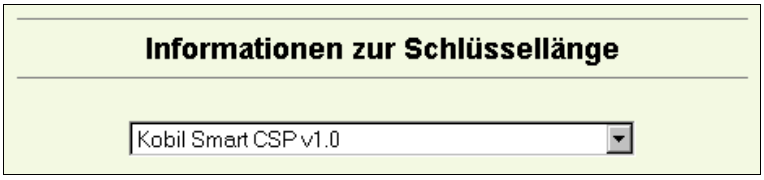

Abbildung 44: Einstellen der Schlüssellänge (Internet Explorer)

b) Betätigen Sie den Button *Absenden*.
Wenn Sie den Netscape Navigator verwenden, erscheint ein neues Fenster, in dem Sie die Smartcard auswählen müssen.

Private Key erstellen - Netscape
Private Key erstellen
Klicken Sie auf "OK". Für Ihr Zertifikat wird nun ein Private Key erstellt
Dies kann einige Minuten dauern.
Wichtig: Wird dieser Vorgang unterbrochen, müssen Sie das Zertifikat erneut anfordern.
Wählen Sie die Karte oder Datenbank, mit der der Schlüssel generiert werden soll:
TCOS 2.0 Chipkarte an COM 1
Mehr Info...
OK
Abbrechen

Abbildung 45: Auswahl des Zertifikatsspeichers (Smartcard)

c) Auf der Antwortseite in Ihrem Browser werden die Zertifikatsdaten angezeigt. Mit Klicken auf den Button *Zertifikat abholen* wird Ihr erneuertes Zertifikat auf die Smartcard geschrieben. Bitte beachten Sie, dass es zu kurzen zeitlichen Verzögerungen kommen kann, da dies ein Online-Prozess ist.

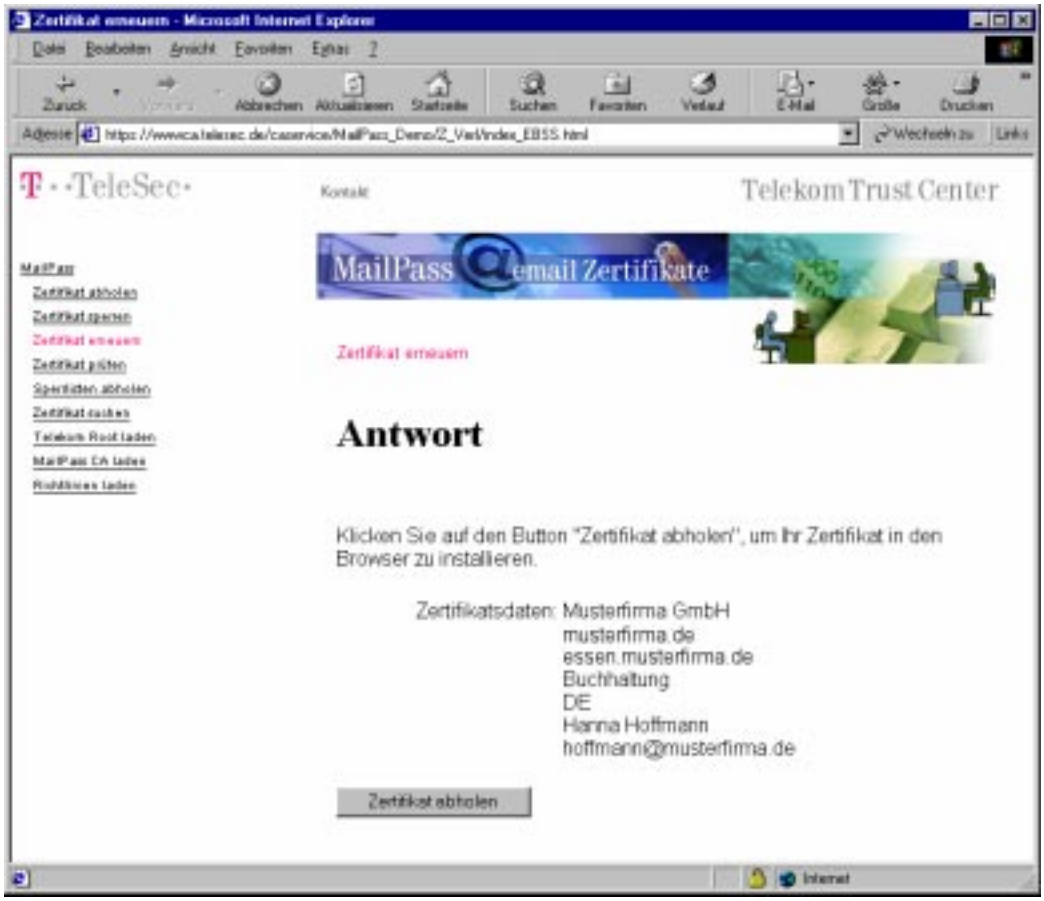

Abbildung 46: Laden des Zertifikats

6) Sie können nun die Smartcard aus dem Smartcard-Leser entfernen.

Beim Einsatz von **Dual Key** ist der Ablauf nahezu identisch. Der einzige Unterschied besteht beim Laden des Zertifikats auf die Smartcard. Hier müssen beide Zertifikate separat durch Klicken der entsprechenden Buttons abgeholt werden.

Nach der Erzeugung Ihres Zertifikats im Telekom Trust Center werden Sie per E-Mail benachrichtigt. Die E-Mail enthält die Referenznummer Ihres Antrags und eine Web-Adresse, über die Sie auch alternativ Ihr Zertifikat abholen können. Eine weitere Alternative ist die Abholung über die (eingeschränkte) Benutzer-Web-Schnittstelle mit der Funktion *Zertifikat abholen*.

5.3.2 Einsatz von Software-PSEs

Dieser Ablauf kann nur durchgeführt werden, wenn Ihr zu erneuerndes Zertifikat gültig ist und mit dem zugehörigen privaten Schlüssel in Ihrem Browser vorliegt.

Prüfen Sie also zunächst, ob sich das Zertifikat in Ihrem Browser befindet:

- Netscape Navigator:
  a) Klicken Sie in der Navigationssymbolleiste Ihres Browsers auf den Button *Sicherheit / Security*.

Trust Center - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop

Abbildung 47: Der Button *Sicherheit* bei Netscape

b) Wählen Sie in der Menüleiste unter *Zertifikate* den Punkt *Eigene*.
c) Über den Button *Anzeigen* können Sie sich die Eigenschaften der dort aufgeführten Zertifikate anschauen. Prüfen Sie anhand der Seriennummer, ob sich das zu erneuernde Zertifikat unter den angezeigten Zertifikaten befindet.

- Microsoft Internet Explorer:
  a) Wählen Sie im Browser-Menü *Extras* den Punkt *Internetoptionen*.

Abbildung 48: Wählen Sie im Menü *Extras* den Punkt *Internetoptionen*

b) Gehen Sie zum Menü *Inhalt* und klicken Sie auf den Button *Zertifikate*.

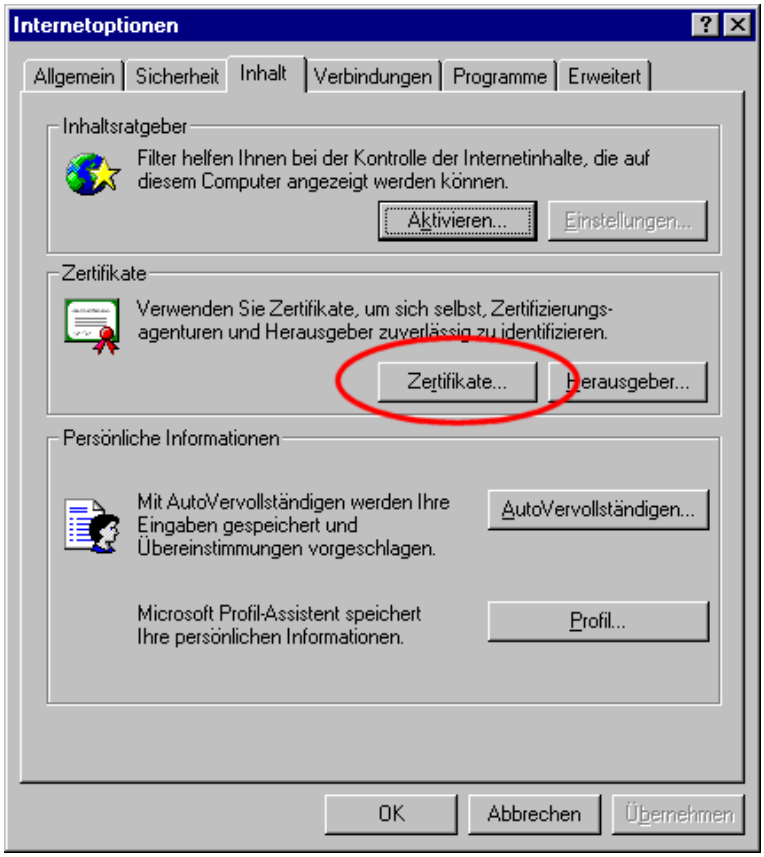

Abbildung 49: Klicken Sie im Menü *Inhalt* auf den Button *Zertifikate*

c) Wählen Sie in der Zertifikatsverwaltung den Punkt *Eigene Zertifikate*.
d) Über den Button *Anzeigen* können Sie sich die Eigenschaften der dort aufgeführten Zertifikate anschauen. Prüfen Sie anhand der Seriennummer, ob sich das zu erneuernde Zertifikat unter den angezeigten Zertifikaten befindet.

Befindet sich Ihr Zertifikat nicht in Ihrem Browser, muss der private Schlüssel über eine Datei (.p12) importiert werden. Dies ist die Datei, die Sie bei der Registrierung erhalten haben.

- Netscape Navigator:
  a) Klicken Sie in der Navigationssymbolleiste Ihres Browsers auf den Button *Sicherheit / Security*.

Abbildung 50: Der Button *Sicherheit* bei Netscape

b) Wählen Sie in der Menüleiste unter *Zertifikate* den Punkt *Eigene*.
c) Klicken Sie auf den Button *Zertifikat importieren*.

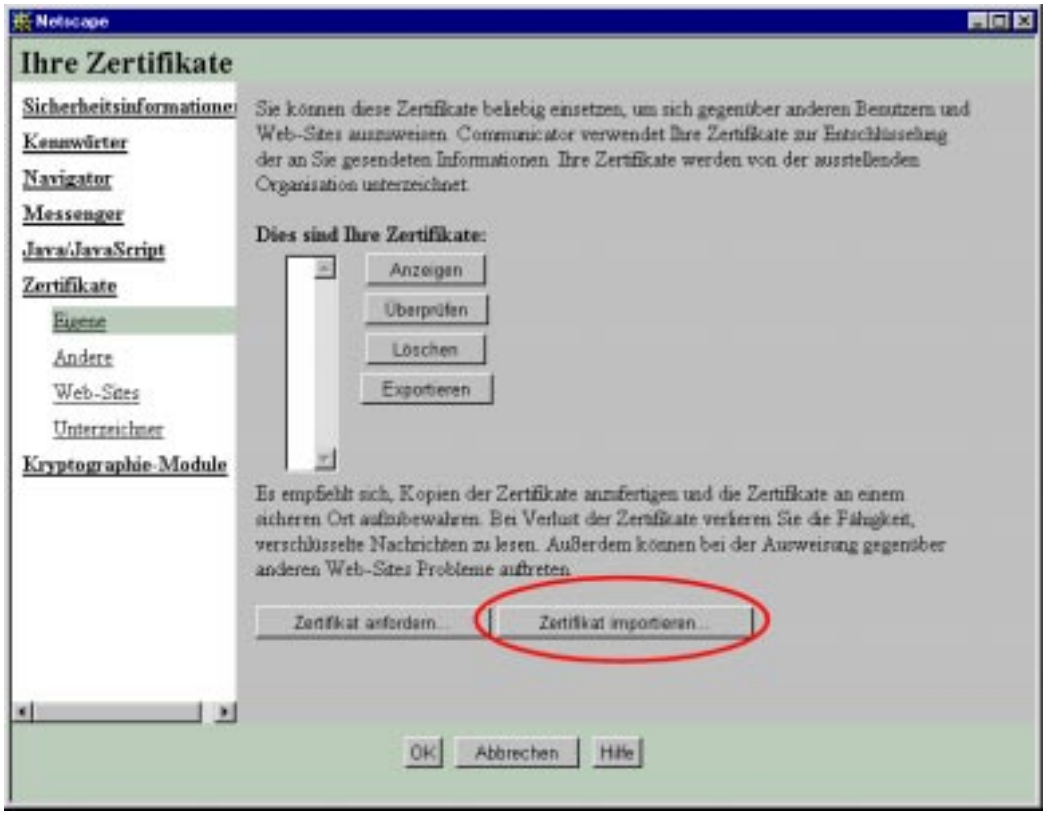
Netscape
Ihre Zertifikate
Sicherheitsinformationen
Kennwörter
Navigator
Messenger
Java/JavaScript
Zertifikate
Eigene
Andere
Web-Sites
Unterzeichner
Kryptographie-Module
Sie können diese Zertifikate beliebig einsetzen, um sich gegenüber anderen Benutzern und Web-Sites auszuweisen. Communicator verwendet Ihre Zertifikate zur Entschlüsselung der an Sie gesendeten Informationen. Ihre Zertifikate werden von der ausstellenden Organisation unterzeichnet.
Dies sind Ihre Zertifikate:
Anzeigen
Überprüfen
Löschen
Exportieren
Es empfiehlt sich, Kopien der Zertifikate anzufertigen und die Zertifikate an einem sicheren Ort aufzubewahren. Bei Verlust der Zertifikate verlieren Sie die Fähigkeit, verschlüsselte Nachrichten zu lesen. Außerdem können bei der Ausweisung gegenüber anderen Web-Sites Probleme auftreten.
Zertifikat anfordern...
Zertifikat importieren...
OK
Abbrechen
Hilfe

Abbildung 51: Zertifikat importieren

d) Geben Sie das Passwort für die Sicherheitsumgebung Ihres Browsers ein.
e) Wählen Sie die Datei aus, die Ihren privaten Schlüssel und das zugehörige Zertifikat enthält. Klicken Sie auf *Öffnen*.
f) Geben Sie das Passwort der Datei ein.
g) Bei erfolgreichem Import erhalten Sie eine entsprechende Meldung.

- Microsoft Internet Explorer:
  a) Wählen Sie im Browser-Menü *Extras* den Punkt *Internetoptionen*.

Abbildung 52: Wählen Sie im Menü *Extras* den Punkt *Internetoptionen*

b) Gehen Sie zum Menü *Inhalt* und klicken Sie auf den Button *Zertifikate*.

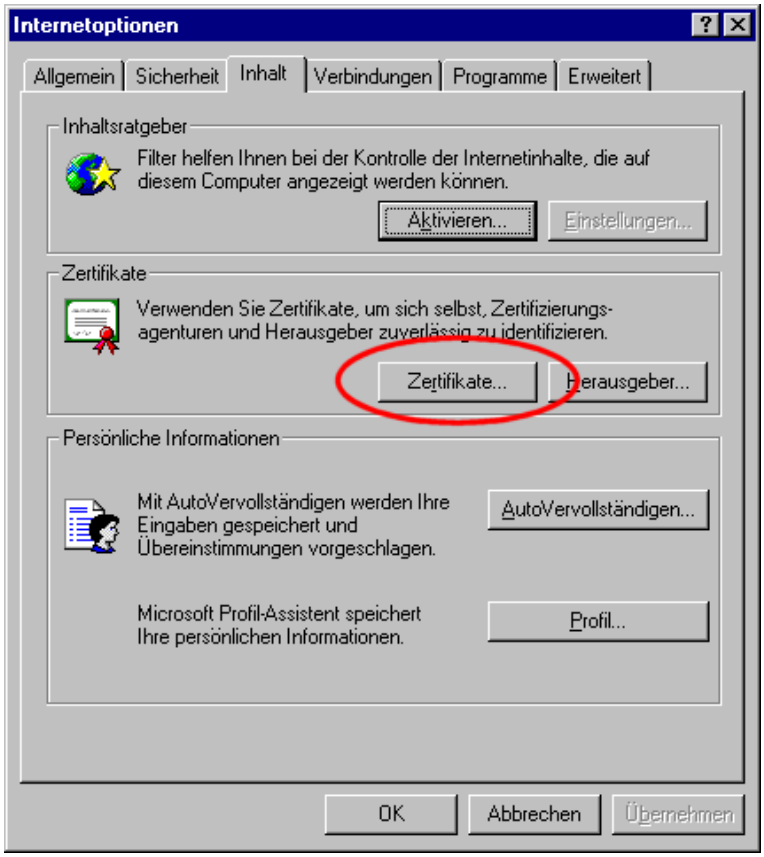

Abbildung 53: Klicken Sie im Menü *Inhalt* auf den Button *Zertifikate*

c) Wählen Sie in der Zertifikatsverwaltung den Punkt *Eigene Zertifikate*.

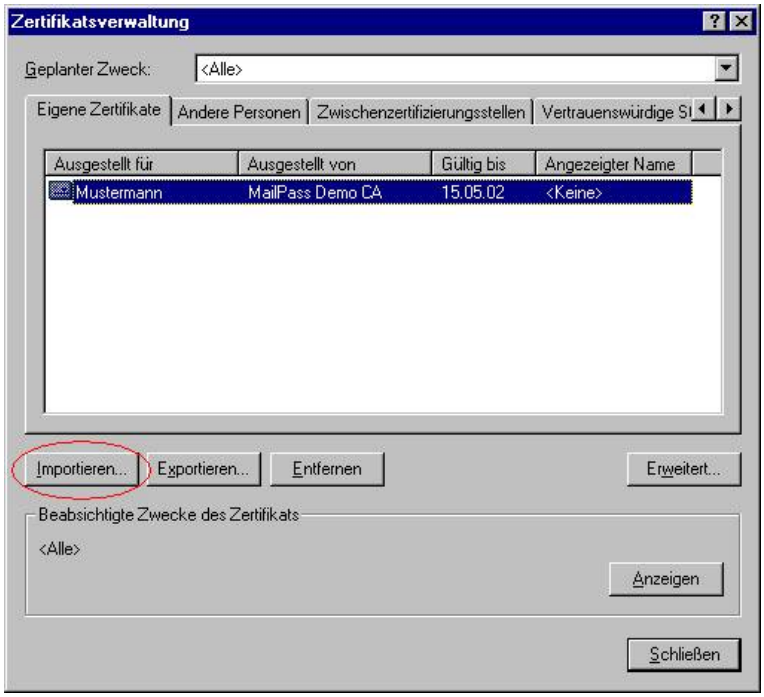

Abbildung 54: Klicken Sie auf den Button *Importieren*

d) Klicken Sie auf den Button *Importieren*.

Import-Assistent für die Zertifikatsverwaltung
Willkommen
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatsvertrauenslisten und -sperrlisten von Ihrem Datenträger in den Zertifikatsspeicher.
Was ist ein Zertifikat?
Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und dient der Bestätigung Ihrer Identität. Zertifikate enthalten Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen.
Was ist ein Zertifikatsspeicher?
Ein Zertifikatsspeicher ist ein Systembereich, in dem Zertifikate, Zertifikatsvertrauenslisten und -sperrlisten gespeichert werden.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen, oder auf "Abbrechen", um den Assistenten zu beenden.
< Zurück
Weiter >
Abbrechen

Abbildung 55: Import-Assistent

e) Es erscheint der Import-Assistent für die Zertifikatsverwaltung. Klicken Sie auf *Weiter*.

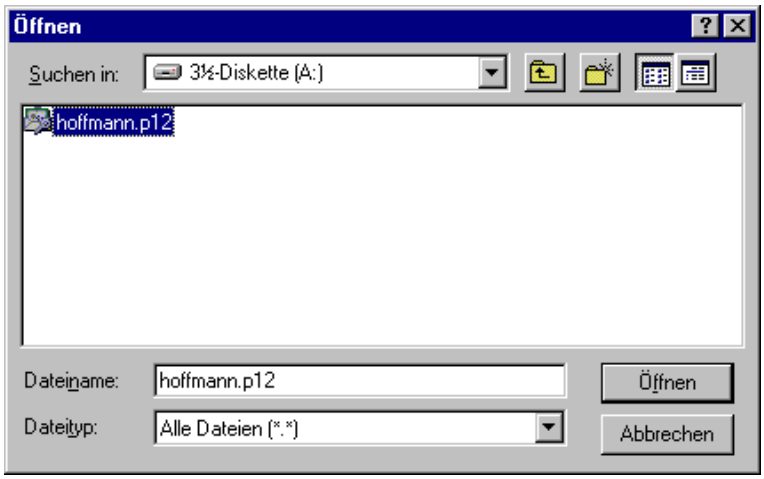

Abbildung 56: Auswahl der zu importierenden Datei

f) Wählen Sie die Datei aus, die Ihren privaten Schlüssel und das zugehörige Zertifikat enthält. Klicken Sie auf *Öffnen*.

Import-Assistent für die Zertifikatsverwaltung
Zertifikatsdatei für den Import
Geben Sie hier die zu importierende Datei an.
Dateiname:
A:\hoffmann.p12
Durchsuchen...
Hinweis: Es können mehrere Zertifikate in einer einzigen Datei in folgenden Formaten gespeichert werden:
Privater Informationsaustausch - PKCS #12 (.PFX)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7b)
Microsoft Speicher serieller Zertifikate (.sst)
< Zurück
Weiter >
Abbrechen

Abbildung 57: Auswahl bestätigen mit *Weiter*

g) Klicken Sie auf *Weiter*.

h) Geben Sie das Passwort der Datei ein. Wählen Sie die Option *Privaten Schlüssel als exportierbar markieren*. Klicken Sie auf *Weiter*.

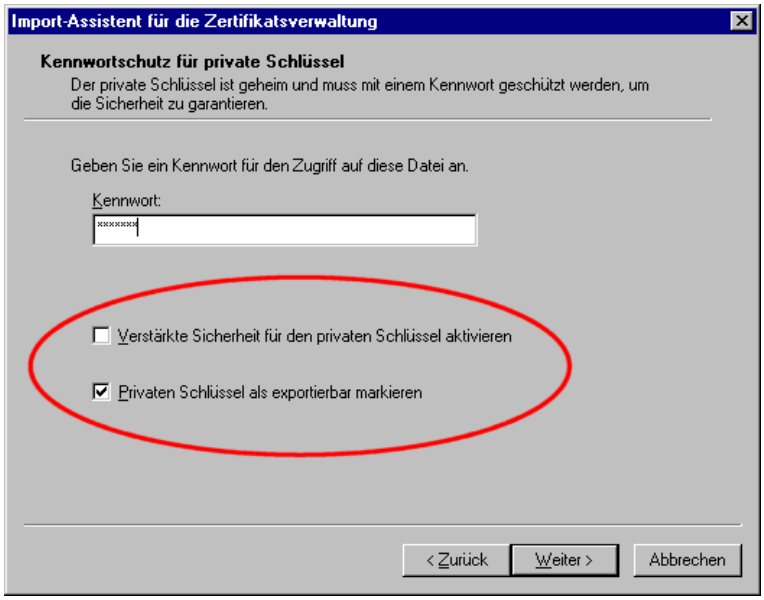
Import-Assistent für die Zertifikatsverwaltung
Kennwortschutz für private Schlüssel
Der private Schlüssel ist geheim und muss mit einem Kennwort geschützt werden, um die Sicherheit zu garantieren.
Geben Sie ein Kennwort für den Zugriff auf diese Datei an.
Kennwort:
Verstärkte Sicherheit für den privaten Schlüssel aktivieren
Privaten Schlüssel als exportierbar markieren
< Zurück
Weiter >
Abbrechen

Abbildung 58: Geben Sie das zugehörige Passwort ein

i) Wählen Sie die Option *Zertifikatsspeicher automatisch auswählen* und klicken Sie auf *Weiter*.

Import-Assistent für die Zertifikatsverwaltung
Zertifikatsspeicher auswählen
Zertifikatsspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Wählen Sie den Zertifikatsspeicher für die neuen Zertifikate.
Zertifikatsspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatsspeicher:
Durchsuchen...
< Zurück
Weiter >
Abbrechen

Abbildung 59: Wählen Sie *Zertifikatsspeicher automatisch wählen*

j) Klicken Sie auf *Fertig stellen*.

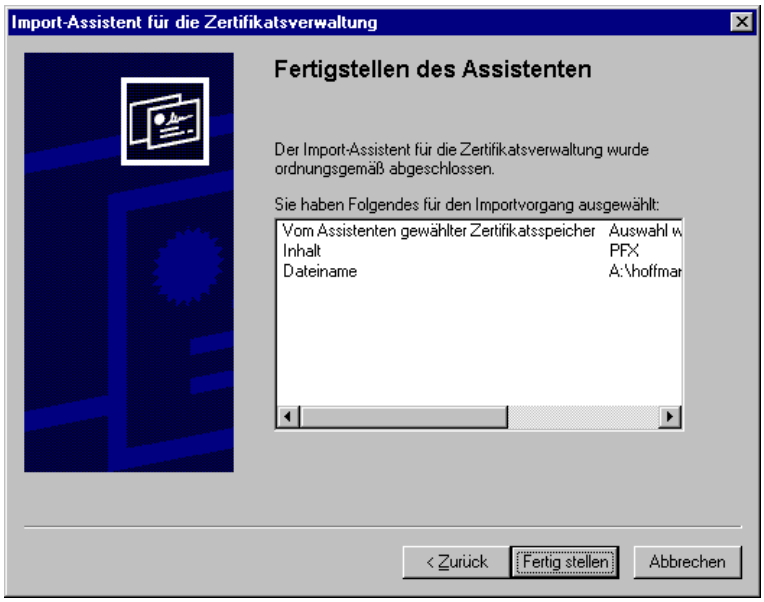

Abbildung 60: Fertigstellung des Imports

k) Bei erfolgreichem Import erhalten Sie eine entsprechende Meldung.

Zertifikatserneuerung: Um Ihr Zertifikat zu erneuern, gehen Sie wie folgt vor:

1) Sie erhalten vom Telekom Trust Center eine E-Mail, in der Sie über den Ablauf Ihres Zertifikats informiert werden.
2) Sie rufen mit Ihrem Browser die Web-Seite der Benutzer-Web-Schnittstelle bzw. der eingeschränkten Benutzer-Web-Schnittstelle auf. Dabei werden Sie aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Diese Daten können Sie dem Informationsblatt entnehmen, welches Sie bei der Registrierung erhalten haben.

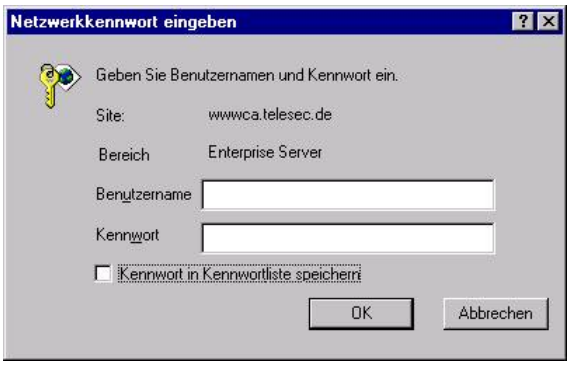

Abbildung 61: Anmeldung mit Benutzername und Passwort

3) Wählen Sie die Funktion *Zertifikat erneuern*. Damit nur Sie in der Lage sind, Ihr Zertifikat zu erneuern, wird eine SSL-Client-Authentifizierung durchgeführt. Hierzu müssen Sie das zu erneuernde Zertifikat aus der angezeigten Liste auswählen. Bei Einsatz des Netscape Navigators wird das Passwort für die Communicator Datenbank abgefragt.

Zertifikat auswählen - Netscape
Zertifikat auswählen
Die Netsite "wwwca.telesec.de" verlangte eine Echtheitsbestätigung des Client-Servers.
Dies ist das Zertifikate der Netsite:
Zertifikat für: Deutsche Telekom AG
Unterzeichnet von: Deutsche Telekom AG
Verschlüsselung: Highest Komplexität (RC4 mit 128-Bit-Verschlüsselung zur Geheimhaltung)
Mehr Info...
Wählen Sie Ihr Zertifikat: Hans Petersen's Deutsche Telekom AG ID
Abbrechen
Weiter

Abbildung 62: Wählen Sie das zu erneuernde Zertifikat aus (Netscape)

Clientauthentifizierung
Identifikation
Die Website, die Sie sich anzeigen lassen möchten, fordert eine Identifikation. Wählen Sie das Zertifikat aus, das für die Verbindung verwendet werden soll.
Hanna Hoffmann
Details...
Zertifikat anzeigen...
OK
Abbrechen

Abbildung 63: Wählen Sie das zu erneuernde Zertifikat aus (Internet Explorer)

4) Es erscheint ein Online-Formular, auf dem Ihnen Ihr Zertifikat angezeigt wird.

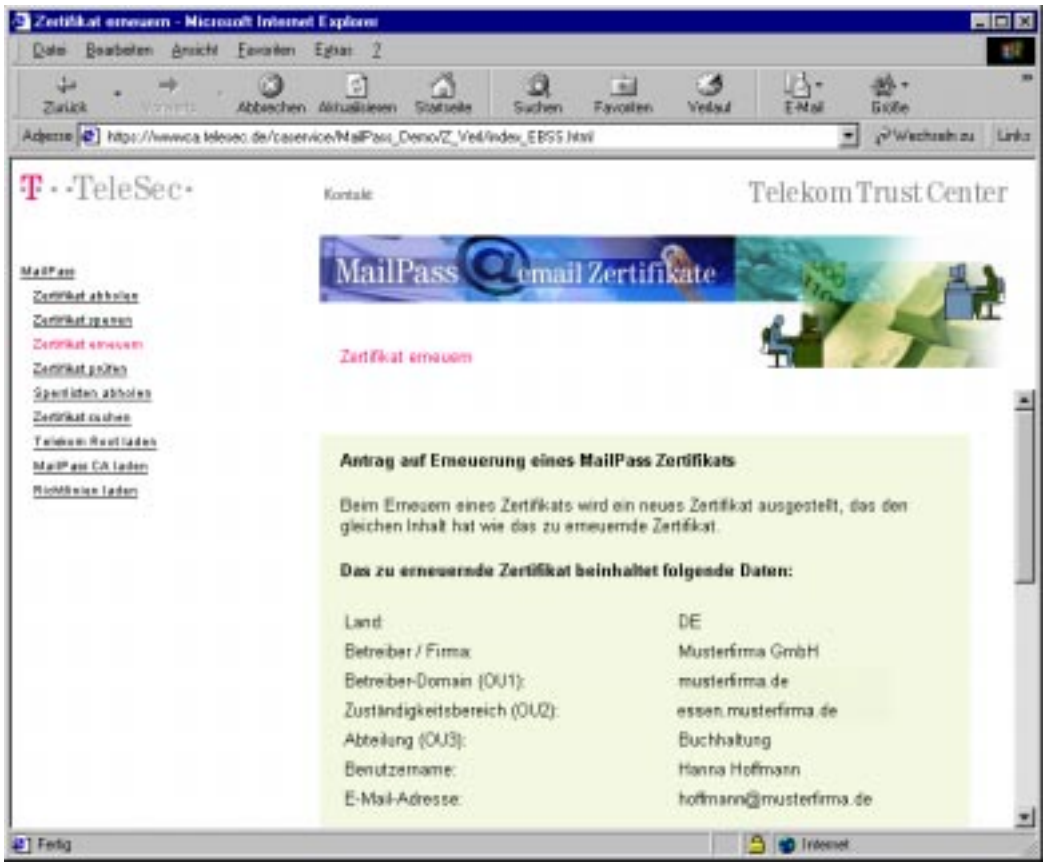
Zertifikat erneuern - Microsoft Internet Explorer
TeleSec
Telekom Trust Center
MailPass email Zertifikate
Zertifikat erneuern
Antrag auf Erneuerung eines MailPass Zertifikats
Beim Erneuern eines Zertifikats wird ein neues Zertifikat ausgestellt, das den gleichen Inhalt hat wie das zu erneuernde Zertifikat.
Das zu erneuernde Zertifikat beinhaltet folgende Daten:
Land: DE
Betreiber / Firma: Musterfirma GmbH
Betreiber-Domain (OU1): musterfirma.de
Zuständigkeitsbereich (OU2): essen.musterfirma.de
Abteilung (OU3): Buchhaltung
Benutzername: Hanna Hoffmann
E-Mail-Adresse: hoffmann@musterfirma.de

Abbildung 64: Anzeige des zu erneuernden Zertifikats

Gehen Sie bitte wie folgt vor:

a) Für das Feld zur Auswahl des Schlüsselgenerators wählen Sie bitte folgende Einstellungen:
   - Netscape Navigator: *1024 (Verschlüsselung hoher Komplexität)*

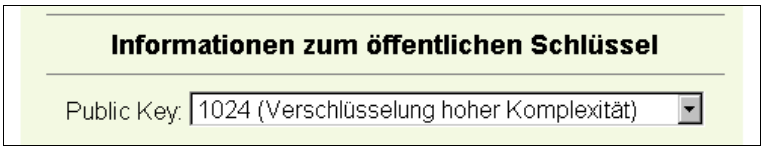

Abbildung 65: Einstellen der Schlüssellänge (Netscape)

   - MS Internet Explorer: *Microsoft Enhanced Cryptographic Provider v1.0*

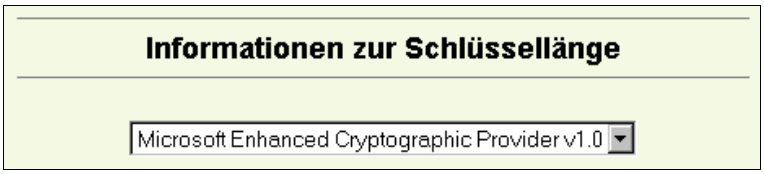

Abbildung 66: Einstellen der Schlüssellänge (Internet Explorer)

b) Klicken Sie auf den Button *Absenden*.
   Wenn Sie den Netscape Navigator verwenden, erscheint ein neues Fenster, in dem Sie die Erzeugung Ihres privaten Schlüssels mit *OK* bestätigen müssen.

Private Key erstellen - Netscape
Private Key erstellen
Klicken Sie auf "OK". Für Ihr Zertifikat wird nun ein Private Key erstellt
Dies kann einige Minuten dauern.
Wichtig: Wird dieser Vorgang unterbrochen, müssen Sie das
Zertifikat erneut anfordern.
Mehr Info...
OK
Abbrechen

Abbildung 67: Start der Schlüsselgenerierung

c) Auf der Antwortseite in Ihrem Browser werden die Zertifikatsdaten angezeigt. Mit Klicken auf den Button *Zertifikat abholen* wird Ihr erneuertes Zertifikat in die Browserdatenbank geschrieben. Bitte beachten Sie, dass es zu kurzen zeitlichen Verzögerungen kommen kann, da dies ein Online-Prozess ist.

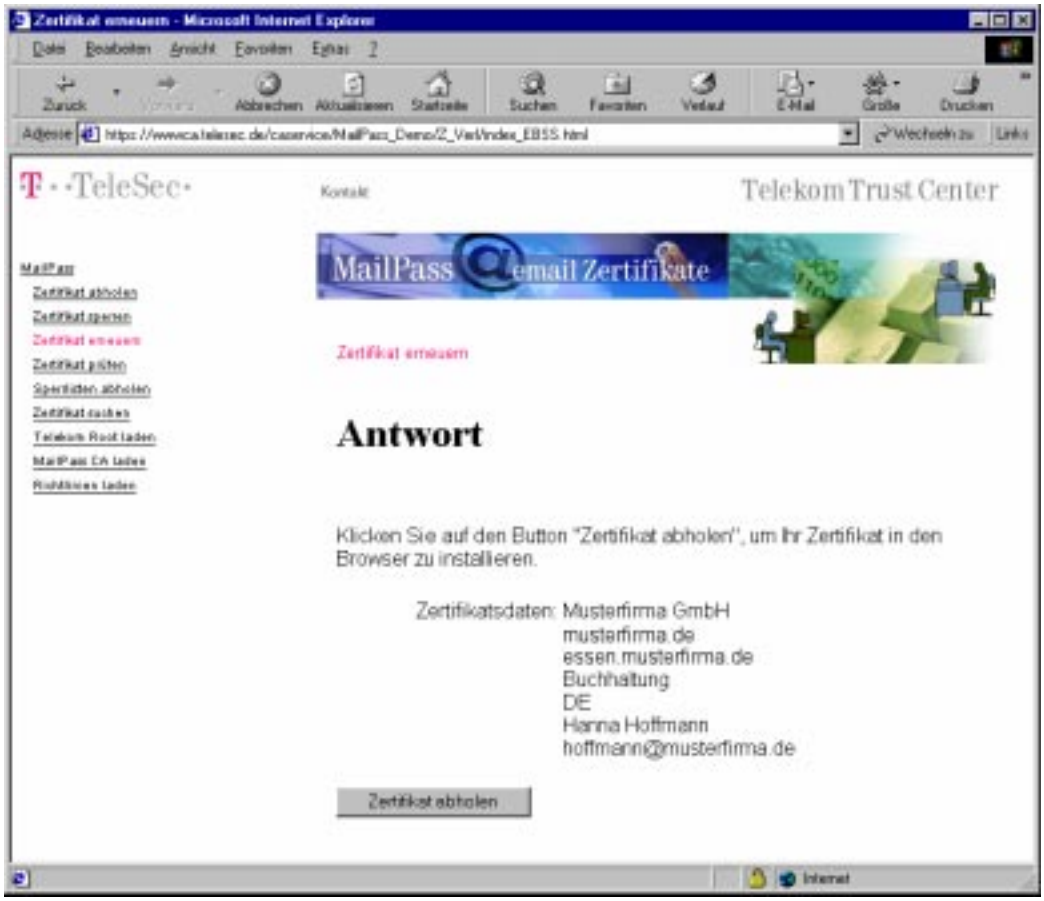

Abbildung 68: Laden des erneuerten Zertifikats

Beim Einsatz von **Dual Key** ist der Ablauf nahezu identisch. Der einzige Unterschied besteht beim Laden des Zertifikats in die Browser-Datenbank. Hier müssen beide Zertifikate separat durch Klicken der entsprechenden Buttons abgeholt werden.

Nach der Erzeugung Ihres Zertifikats im Telekom Trust Center werden Sie per E-Mail benachrichtigt. Die E-Mail enthält die Referenznummer Ihres Antrags und eine Web-Adresse, über die Sie auch alternativ Ihr Zertifikat abholen können. Eine weitere Alternative ist die Abholung über die (eingeschränkte) Benutzer-Web-Schnittstelle mit der Funktion *Zertifikat abholen*.

Um Ihren privaten Schlüssel und das Zertifikat in Ihre Client-Anwendung importieren zu können, müssen Sie Ihren privaten Schlüssel und das Zertifikat noch aus dem Browser in eine PKCS#12-Datei exportieren. Dieser Ablauf ist in Kapitel 5.5 beschrieben.

5.4 Weitere Prozesse

Über die Funktionen zum Beantragen, Sperren und Erneuern von Zertifikaten hinaus stehen Ihnen über die Benutzer-Web-Schnittstelle bzw. die eingeschränkte Benutzer-Web-Schnittstelle weitere Funktionen zur Verfügung. Diese werden im Folgenden beschrieben.

5.4.1 Zertifikat suchen

Diese Funktion ermöglicht Ihnen die Suche nach einem Zertifikat im Verzeichnisdienst von T-TeleSec MailPass. Die E-Mail-Adresse des Zertifikatsbesitzers wird hierbei als Suchkriterium verwendet.

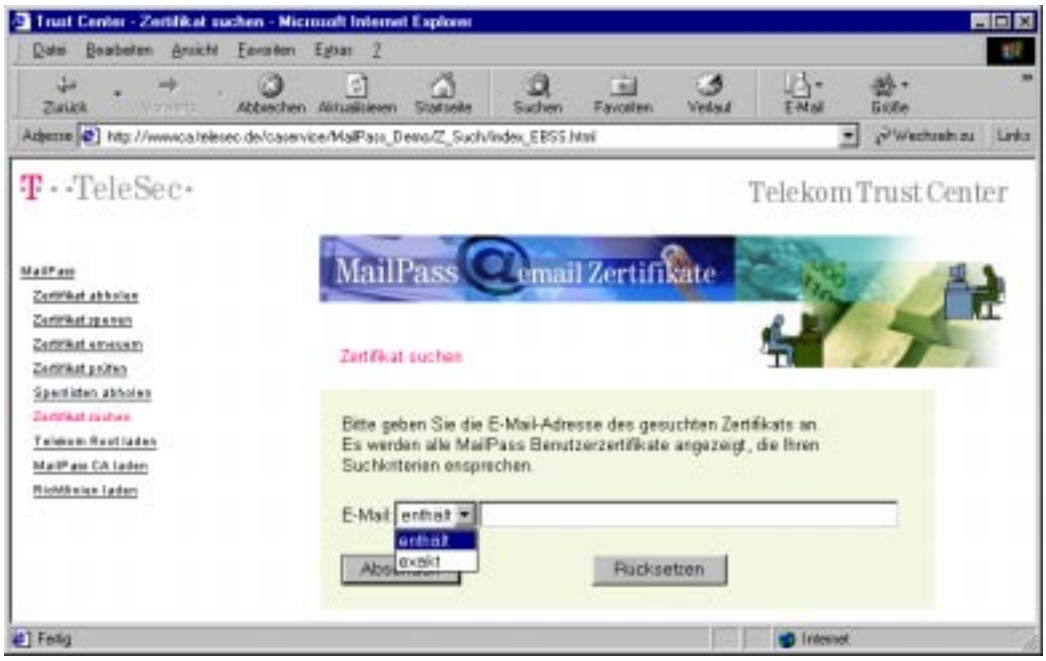

Abbildung 69: Zertifikat im Verzeichnisdienst suchen

Man kann bei der Suche auswählen, ob nach der exakten oder nur einem Teil der E-Mail-Adresse gesucht werden soll.

Abbildung 70: Suchergebnis

Das gefundene Zertifikat kann ausgewählt und in den Browser importiert werden. Die genaue Vorgehensweise für den Import von Zertifikaten in *Netscape Navigator* und *Microsoft Internet Explorer* ist in Abschnitt 5.4.4 beschrieben.

5.4.2 Zertifikat prüfen

Diese Funktion erlaubt es Ihnen, die Gültigkeit eines Zertifikats zu überprüfen. Geben Sie in das vorgesehene Feld die Seriennummer des zu prüfenden Zertifikats ein.

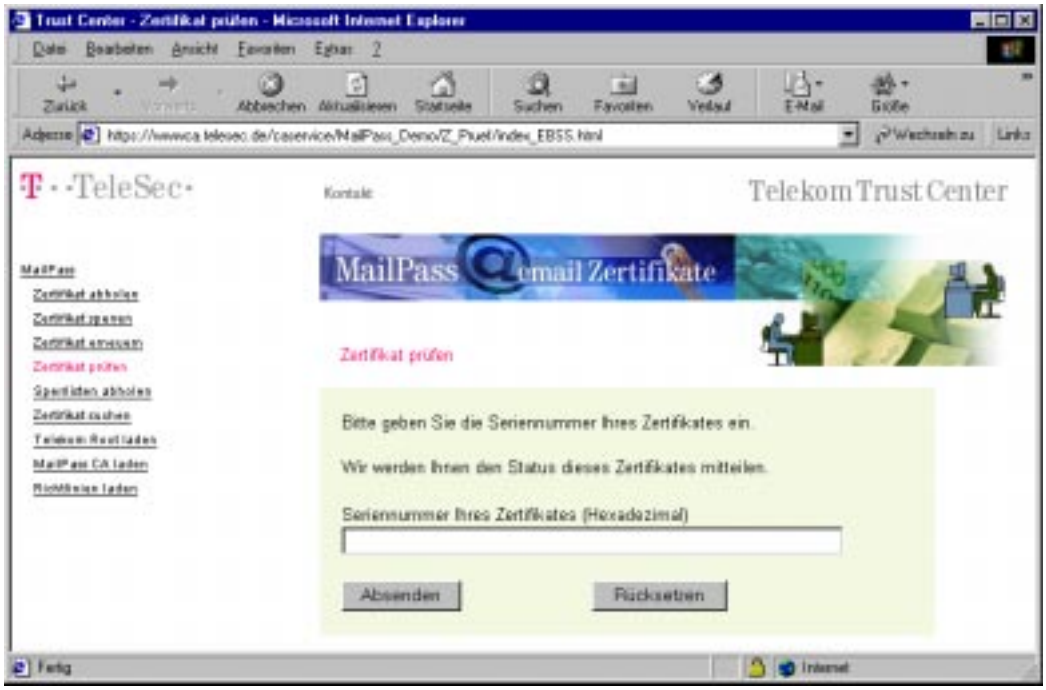
Trust Center - Zertifikat prüfen - Microsoft Internet Explorer
TeleSec
Telekom Trust Center
MailPass email Zertifikate
Zertifikat prüfen
Bitte geben Sie die Seriennummer Ihres Zertifikates ein.
Wir werden Ihnen den Status dieses Zertifikates mitteilen.
Seriennummer Ihres Zertifikates (Hexadezimal)
Absenden
Rücksetzen

Abbildung 71: Geben Sie die Seriennummer des zu prüfenden Zertifikats an

Als Antwort erhalten Sie Informationen über den Status des Zertifikats.

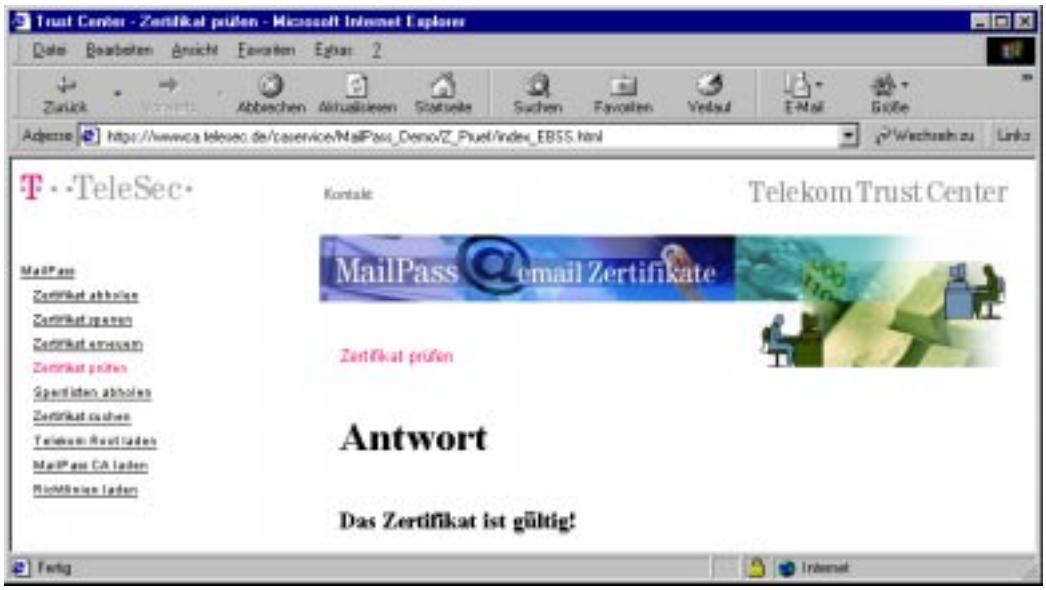

Abbildung 72: Statusinformationen des Zertifikats

5.4.3 Sperrlisten abholen

Die Sperrung von Zertifikaten wird über eine Sperrliste bekannt gemacht. Mit der Funktion *Sperrliste abholen* können Sie eine aktuelle Version der Sperrliste von gesperrten Benutzerzertifikaten (CRL, Certificate Revocation List) und gesperrten CA-Zertifikaten (ARL, Authority Revocation List) downloaden.

Wählen Sie zunächst aus, ob Sie die ARL (Deutsche Telekom Root CA) oder die CRL (Mail Pass CA) laden wollen. Klicken Sie zum Laden der Sperrliste auf den Button *Sperrliste abholen*.

Hinweis: Der Netscape Navigator 4.x kann keine ARLs auswerten. Beim Versuch, die ARL zu laden erscheint eine Fehlermeldung.

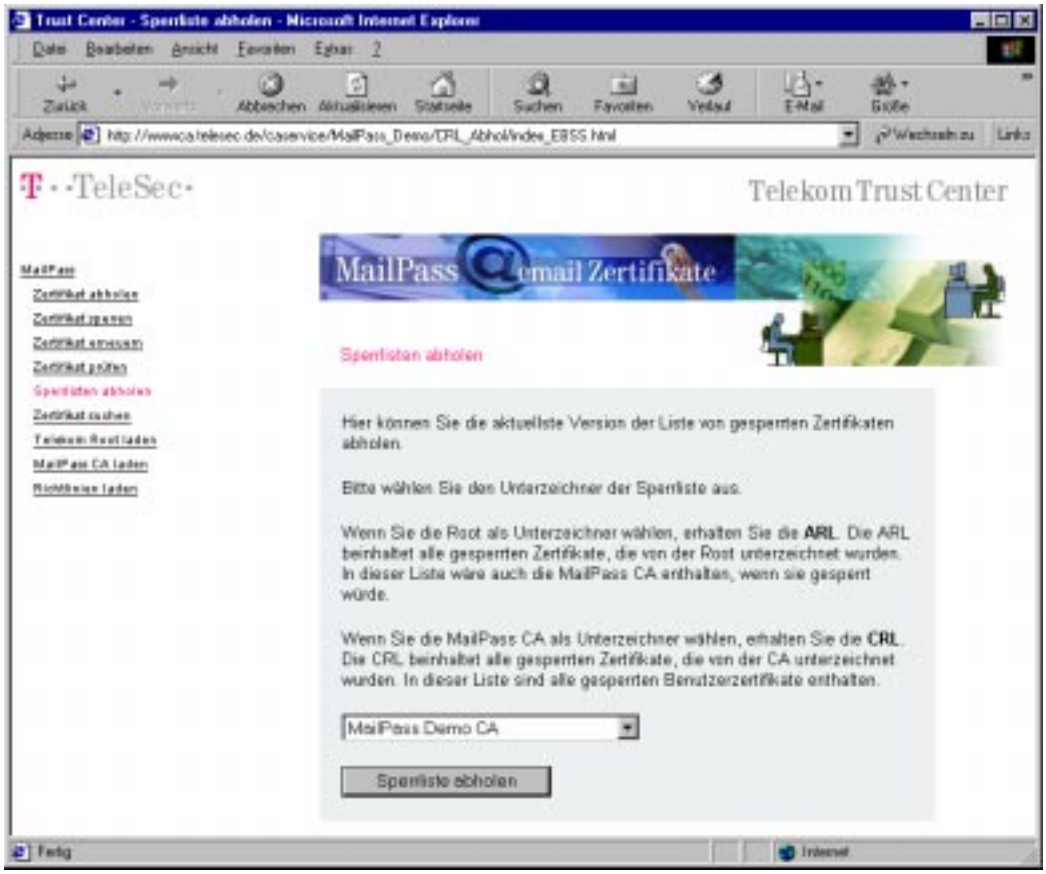
Trust Center - Sperrliste abholen - Microsoft Internet Explorer
TeleSec
Telekom Trust Center
MailPass
email Zertifikate
Sperrlisten abholen
Hier können Sie die aktuellste Version der Liste von gesperrten Zertifikaten abholen.
Bitte wählen Sie den Unterzeichner der Sperrliste aus.
Wenn Sie die Root als Unterzeichner wählen, erhalten Sie die ARL. Die ARL beinhaltet alle gesperrten Zertifikate, die von der Root unterzeichnet wurden. In dieser Liste wäre auch die MailPass CA enthalten, wenn sie gesperrt würde.
Wenn Sie die MailPass CA als Unterzeichner wählen, erhalten Sie die CRL. Die CRL beinhaltet alle gesperrten Zertifikate, die von der CA unterzeichnet wurden. In dieser Liste sind alle gesperrten Benutzerzertifikate enthalten.
MailPass Demo CA
Sperrliste abholen

Abbildung 73: Abholen der aktuellen Sperrliste

- **Netscape Navigator:** Die Sperrliste wird direkt in den Browser geladen. Sie können sich die Sperrliste wie folgt anzeigen lassen:
  a) Klicken Sie in der Navigationssymbolleiste Ihres Browsers auf den Button *Sicherheit*.
  b) Wählen Sie in der Menüleiste unter *Zertifikate* den Punkt *Unterzeichner*.
  c) Klicken Sie auf den Button *CRLs anzeigen/bearbeiten*.

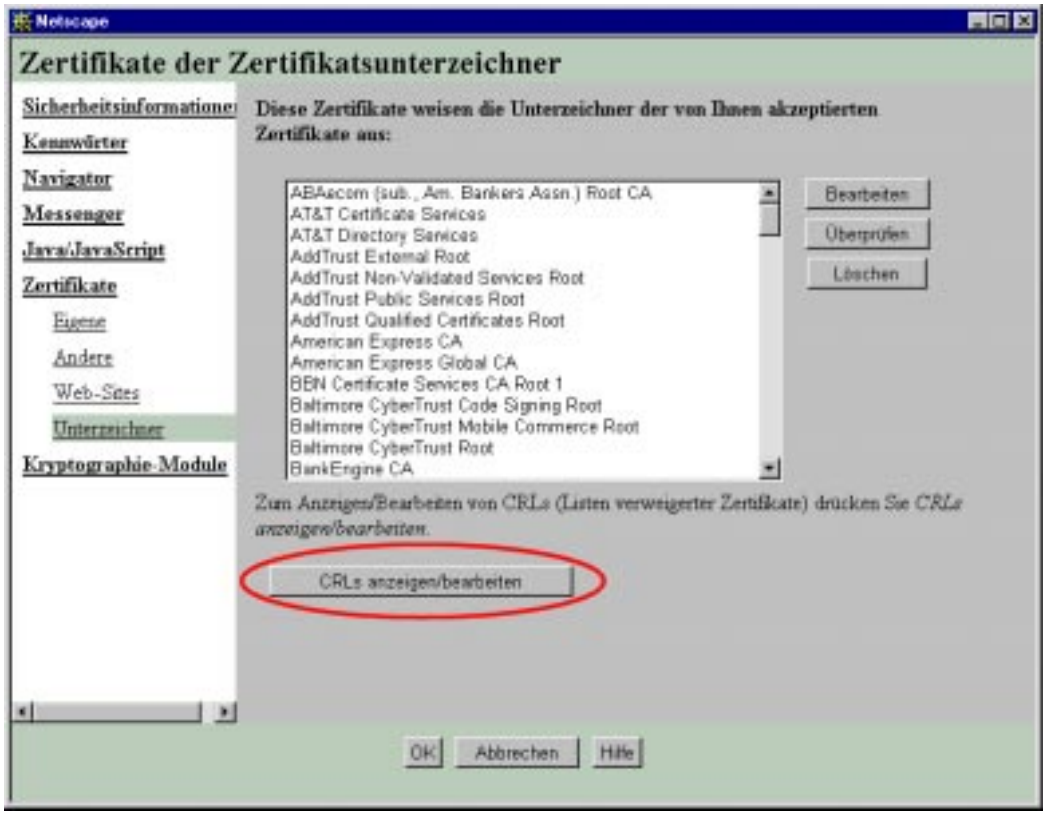

Abbildung 74: Klicken Sie auf den Button *CRLs anzeigen/bearbeiten*

d) Wählen Sie die Sperrliste der MailPass CA aus.

Abbildung 75: Auswahl der MailPass-CRL

e) Durch Klick auf den Button *Mehr Info...* können Sie sich die Liste der gesperrten Zertifikate ansehen.

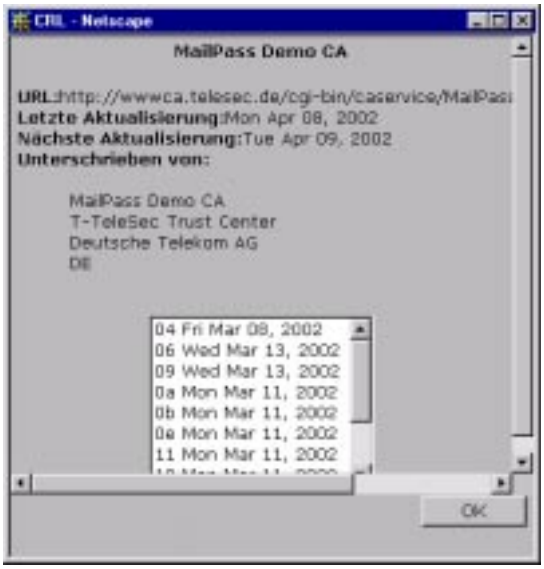

Abbildung 76: Inhalt der Sperrliste sind die Seriennummern der gesperrten Zertifikate und der Zeitpunkt der Sperrung

- **Microsoft Internet Explorer:** Sie haben zwei Optionen:

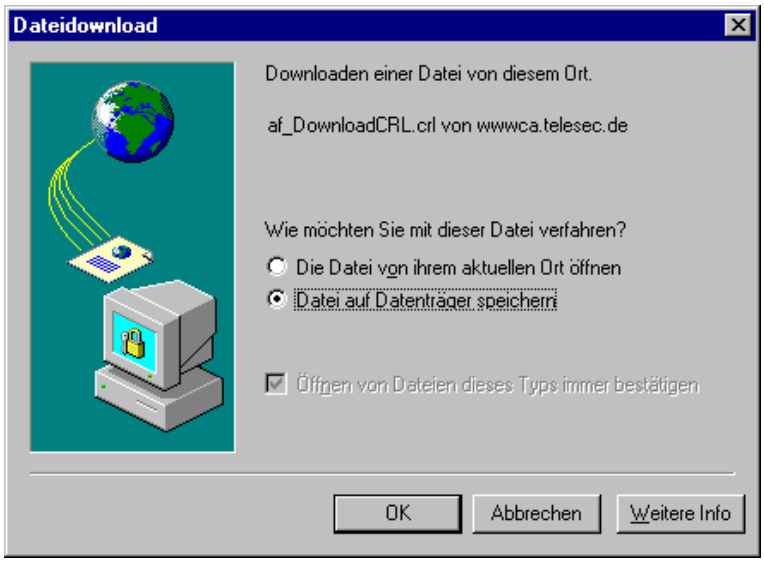

Abbildung 77: Wählen Sie *Öffnen* oder *Speichern*

- *Die Datei von Ihrem aktuellen Ort öffnen*: Die Zertifikatssperrliste wird Ihnen direkt angezeigt.

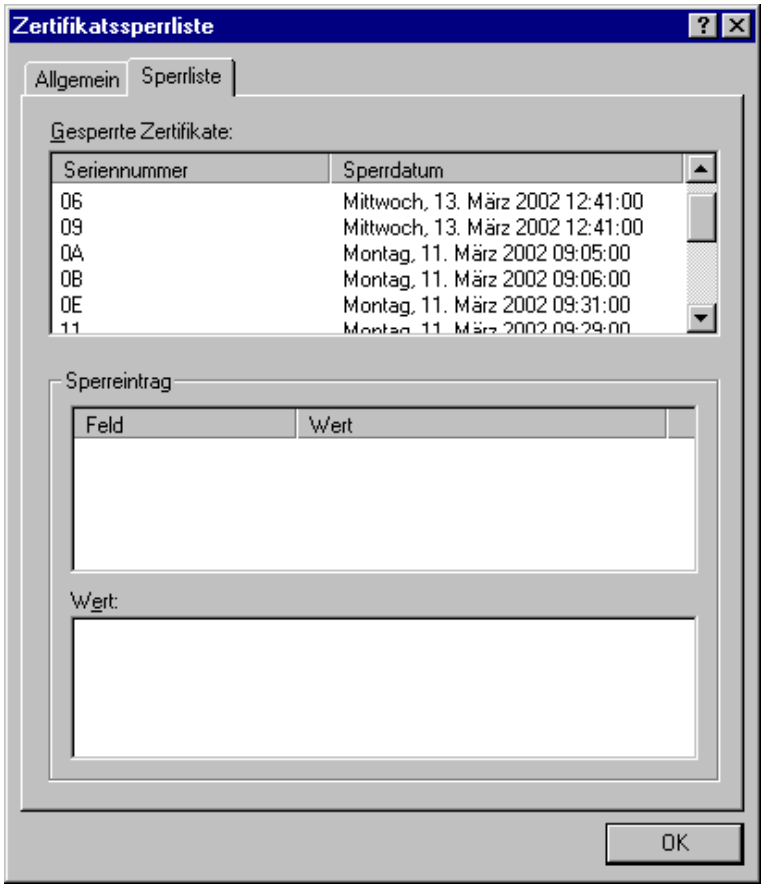

Abbildung 78: Die Sperrliste wird Ihnen direkt angezeigt

- *Datei auf Datenträger speichern*: Geben Sie einen Speicherplatz für die Sperrliste an.

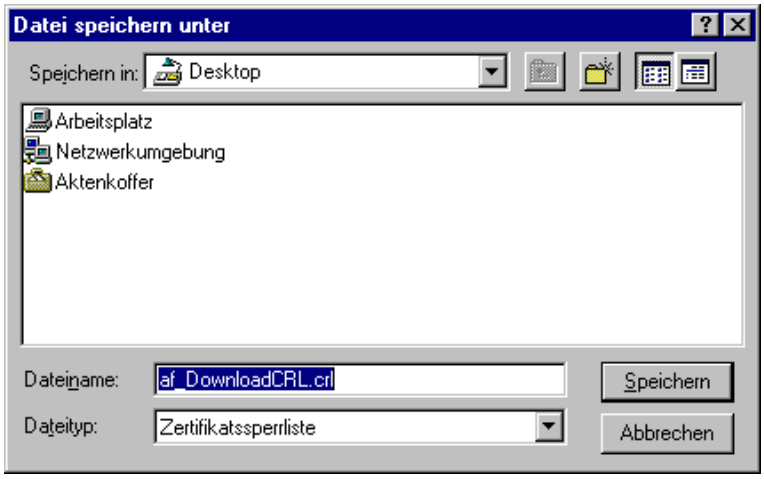

Abbildung 79: Geben Sie einen Speicherplatz für die Sperrliste an

Durch Öffnen dieser Datei (.crl) können Sie sich die Zertifikatssperrliste anzeigen lassen.

5.4.4 Telekom Root laden

Mit dieser Funktion können Sie sich das Zertifikat der obersten Telekom-Zertifizierungsinstanz anzeigen lassen.

- **Netscape Navigator:** Durch Klicken auf den Link *Download* wird das Zertifikat in Ihrem Browser gespeichert.

- **Microsoft Internet Explorer:** Sie haben zwei Optionen:

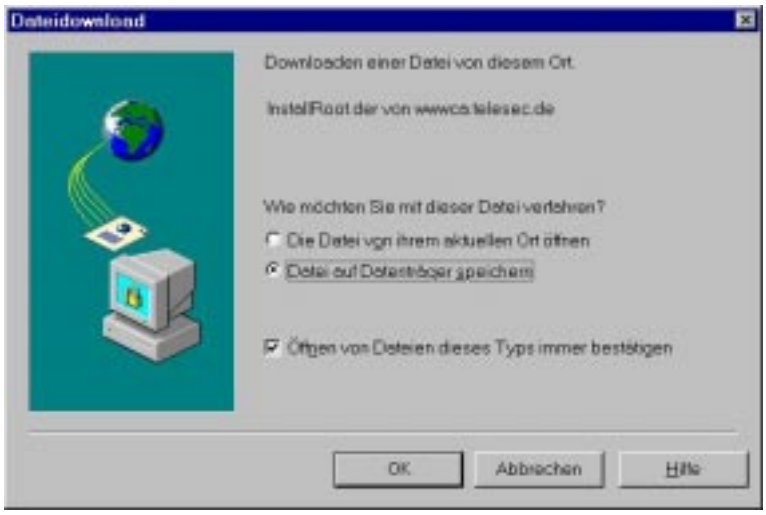

Abbildung 80: Wählen Sie *Öffnen* oder *Speichern*

- *Die Datei von Ihrem aktuellen Ort öffnen*: Das Zertifikat wird Ihnen direkt angezeigt, mit der Option es in Ihren Browser zu importieren.

Abbildung 81: Ansicht des Zertifikats

- *Datei auf Datenträger speichern*: Geben Sie einen Speicherplatz für das Zertifikat an.

Abbildung 82: Geben Sie einen Speicherplatz für das Zertifikat ein

Durch Öffnen dieser Datei (.der) können Sie sich das Zertifikat anzeigen lassen, mit der Option es in Ihren Browser zu importieren.

Hinweis: Je nach eingesetzter Browserversion lautet die Endung der Datei möglicherweise nicht „.der“. In diesem Fall müssen Sie die Endung vor dem Öffnen der Datei in „.der“ umbenennen.

5.4.5 MailPass CA Zertifikat laden

Mit dieser Funktion können Sie sich das Zertifikat der Zertifizierungsinstanz anzeigen lassen, welche Ihr MailPass-Zertifikat ausgestellt hat. Durch Klicken auf den Link *Download* können Sie das Zertifikat in Ihren Browser integrieren. Das Vorgehen ist identisch mit dem in Kapitel 5.4.4 beschriebenen Umgang mit dem Zertifikat der Telekom Root CA.

5.4.6 Richtlinien laden

Über diesen Menüpunkt können Sie das CPS (Certification Practice Statement) für T-TeleSec MailPass downloaden. Dieses Dokument enthält die Richtlinien für den Betrieb der MailPass CA und Regeln für den Umgang mit den von dieser CA ausgestellten Zertifikate.

Das Dokument liegt im PDF-Format vor. Um es öffnen zu können, benötigen Sie den Adobe Acrobat Reader.

5.5 Export einer PKCS#12-Datei

Um Ihren privaten Schlüssel und das Zertifikat in Ihre Anwendungs-Software importieren zu können, müssen Sie Schlüssel und Zertifikat zunächst aus dem Browser in einer Datei (*.p12) speichern. Dieser Vorgang ist je nach eingesetztem Browser verschieden.

5.5.1 Netscape Navigator

1) Klicken Sie in der Navigationssymbolleiste Ihres Browsers auf den Button *Sicherheit / Security*.

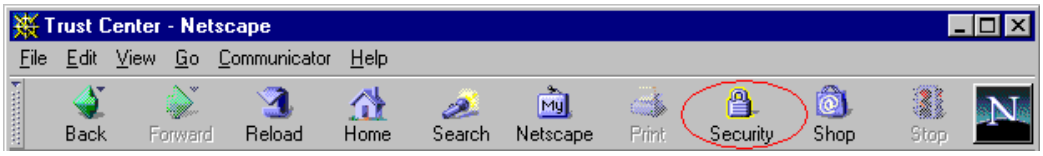
Trust Center - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop

Abbildung 83: Der Button *Sicherheit* bei Netscape

2) Wählen Sie in der Menüleiste unter Zertifikate den Punkt *Eigene*.
3) Wählen Sie aus den dort angezeigten Zertifikaten das aktuell von der MailPass CA ausgestellte Zertifikat.

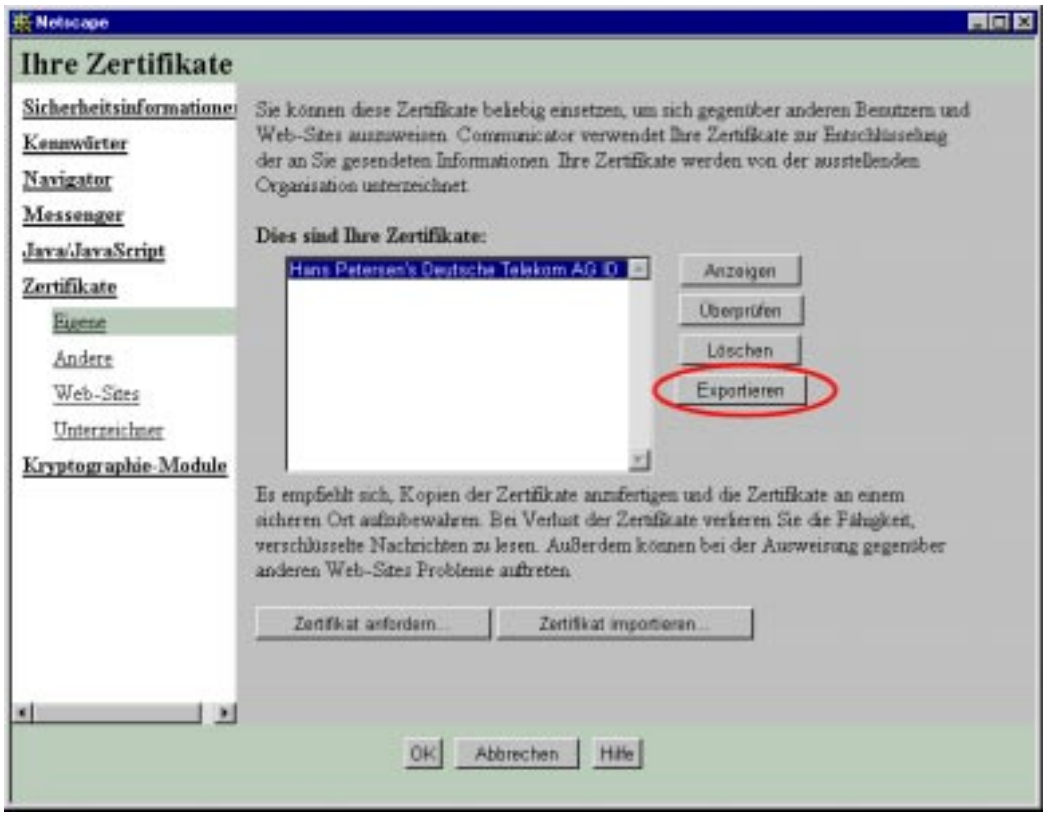
Netscape
Ihre Zertifikate
Sicherheitsinformationen
Kennwörter
Navigator
Messenger
Java/JavaScript
Zertifikate
Eigene
Andere
Web-Sites
Unterzeichner
Kryptographie-Module
Sie können diese Zertifikate beliebig einsetzen, um sich gegenüber anderen Benutzern und Web-Sites auszuweisen. Communicator verwendet Ihre Zertifikate zur Entschlüsselung der an Sie gesendeten Informationen. Ihre Zertifikate werden von der ausstellenden Organisation unterzeichnet.
Dies sind Ihre Zertifikate:
Hans Petersen's Deutsche Telekom AG ID
Anzeigen
Überprüfen
Löschen
Exportieren
Es empfiehlt sich, Kopien der Zertifikate anzufertigen und die Zertifikate an einem sicheren Ort aufzubewahren. Bei Verlust der Zertifikate verlieren Sie die Fähigkeit, verschlüsselte Nachrichten zu lesen. Außerdem können bei der Ausweisung gegenüber anderen Web-Sites Probleme auftreten.
Zertifikat anfordern...
Zertifikat importieren...
OK
Abbrechen
Hilfe

Abbildung 84: Wählen Sie das zu exportierende Zertifikat aus

4) Klicken Sie auf den Button *Exportieren*. (Sollte Netscape anschließend mehrere Zertifikate unter der ausgewählten Zertifikatsbezeichnung darstellen, markieren Sie anhand der dargestellten Gültigkeitsdauer das aktuellste).
5) Das Passwort für die Sicherheitsumgebung Ihres Browsers wird abgefragt. Klicken Sie anschließend auf *OK*.
6) Geben Sie nun ein Passwort ein, mit dem die Datei geschützt wird, in der Sie Ihren privaten Schlüssel und das Zertifikat speichern. Beachten Sie dabei bitte die Passwortregeln in Kapitel 6.2. Klicken Sie anschließend auf *OK*.

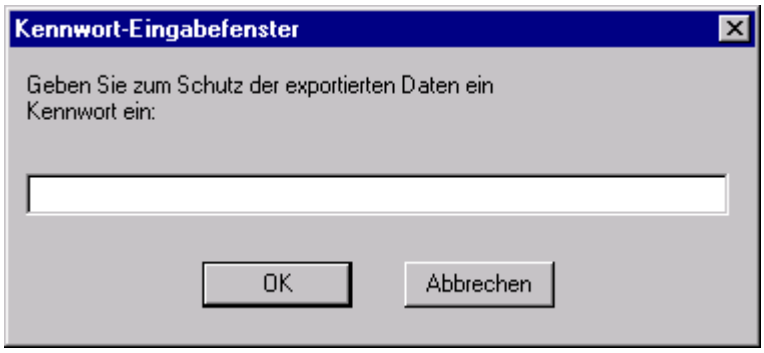

Abbildung 85: Eingabe des Passworts für die Datei

7) Bestätigen Sie das zuletzt eingegebene Passwort und klicken Sie anschließend auf *OK*.
8) Geben Sie die Datei an, in der ihr privater Schlüssel und das Zertifikat gespeichert werden sollen.

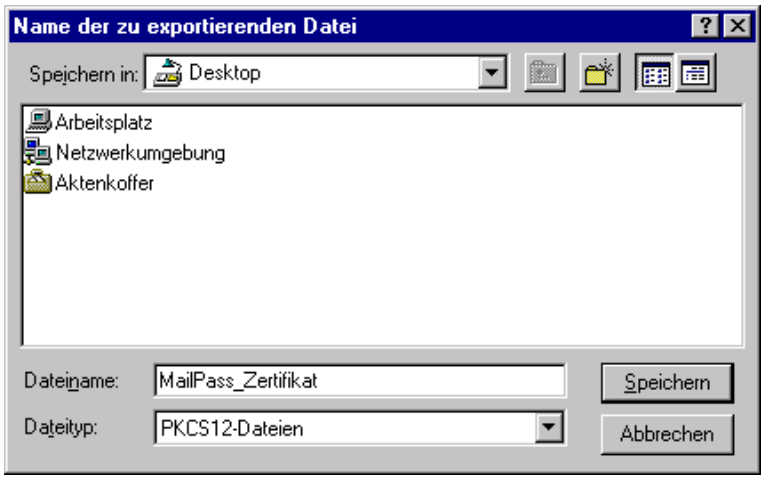

Abbildung 86: Angabe des Dateinamen und Speicherortes

5.5.2 Microsoft Internet Explorer

1) Wählen Sie im Browser-Menü *Extras* den Punkt *Internetoptionen*.

Abbildung 87: Wählen Sie im Menü *Extras* den Punkt *Internetoptionen*

2) Gehen Sie zum Menü *Inhalt* und klicken Sie auf den Button *Zertifikate*.

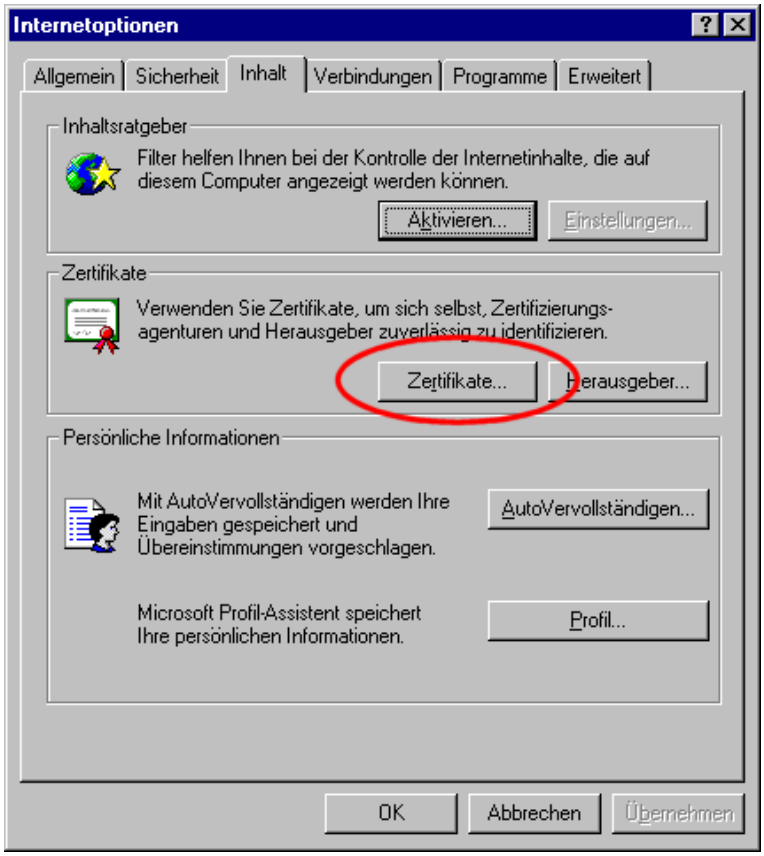

Abbildung 88: Klicken Sie im Menü *Inhalt* auf den Button *Zertifikate*

Sie befinden sich nun in der Zertifikatsverwaltung. Markieren Sie in der Liste *Eigene Zertifikate* das von der MailPass CA aktuell ausgestellte Zertifikat und klicken Sie auf den Button *Exportieren*.

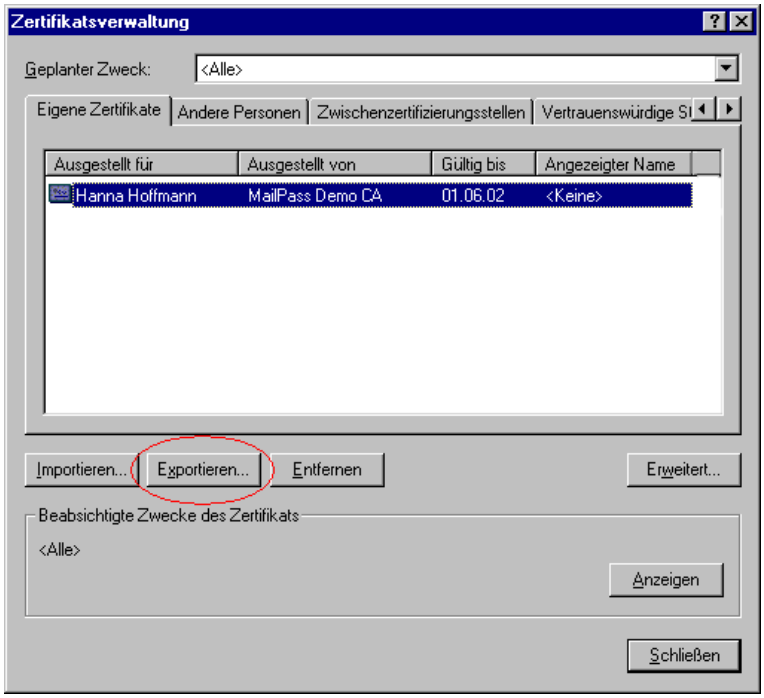

Abbildung 89: Wählen Sie das zu exportierende Zertifikat

3) Es erscheint der Export-Assistent für die Zertifikatsverwaltung. Klicken Sie auf *Weiter*.

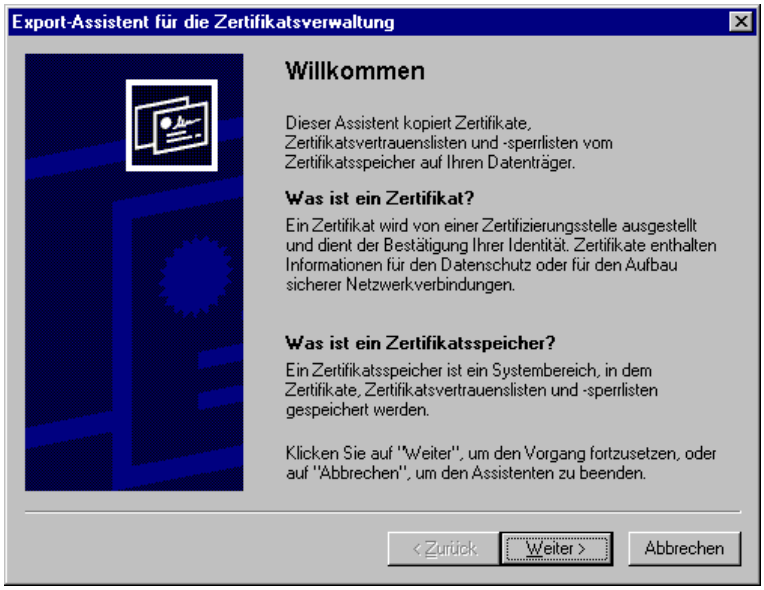
Export-Assistent für die Zertifikatsverwaltung
Willkommen
Dieser Assistent kopiert Zertifikate, Zertifikatsvertrauenslisten und -sperrlisten vom Zertifikatsspeicher auf Ihren Datenträger.
Was ist ein Zertifikat?
Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und dient der Bestätigung Ihrer Identität. Zertifikate enthalten Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen.
Was ist ein Zertifikatsspeicher?
Ein Zertifikatsspeicher ist ein Systembereich, in dem Zertifikate, Zertifikatsvertrauenslisten und -sperrlisten gespeichert werden.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen, oder auf "Abbrechen", um den Assistenten zu beenden.
< Zurück
Weiter >
Abbrechen

Abbildung 90: Export-Assistent

4) Wählen Sie die Option *Ja, privaten Schlüssel exportieren* und klicken Sie auf *Weiter*.

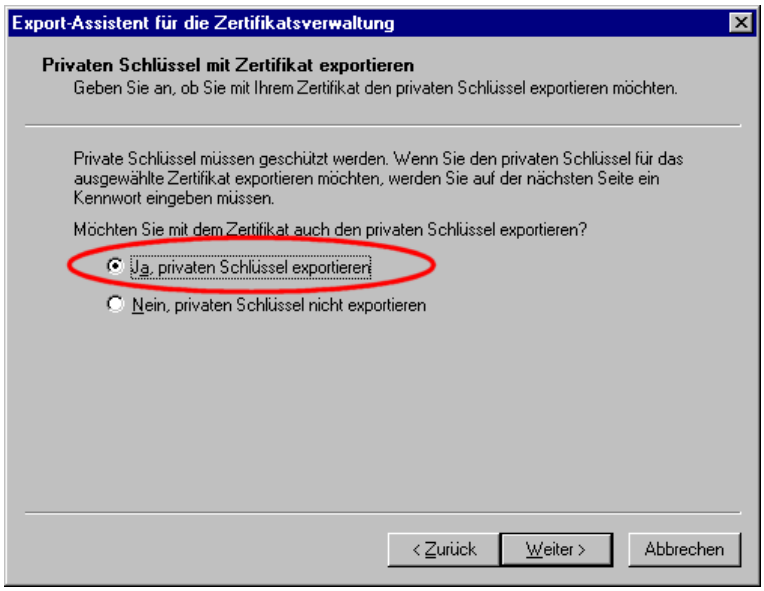
Export-Assistent für die Zertifikatsverwaltung
Privaten Schlüssel mit Zertifikat exportieren
Geben Sie an, ob Sie mit Ihrem Zertifikat den privaten Schlüssel exportieren möchten.
Private Schlüssel müssen geschützt werden. Wenn Sie den privaten Schlüssel für das ausgewählte Zertifikat exportieren möchten, werden Sie auf der nächsten Seite ein Kennwort eingeben müssen.
Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?
Ja, privaten Schlüssel exportieren
Nein, privaten Schlüssel nicht exportieren
< Zurück
Weiter >
Abbrechen

Abbildung 91: Option *Ja, privaten Schlüssel exportieren* wählen

5) Wählen Sie die Optionen wie in Abbildung 92 angegeben und klicken Sie auf *Weiter*.

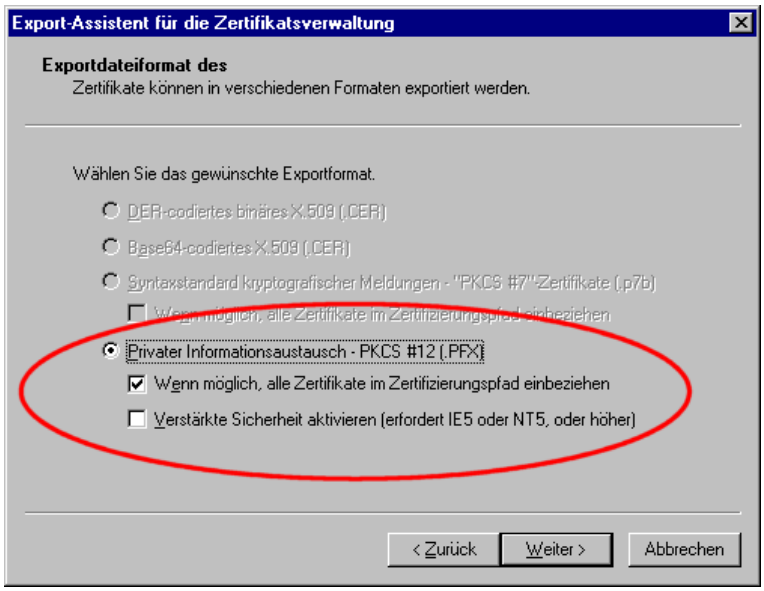

Abbildung 92: Wählen Sie die Optionen wie angegeben

6) Geben Sie nun ein Passwort ein, mit dem die Datei geschützt wird, in der Sie Ihren privaten Schlüssel und das Zertifikat speichern. Beachten Sie dabei bitte die Passwortregeln in Kapitel 6.2. Bestätigen Sie das Passwort. Klicken Sie auf *Weiter*.

Export-Assistent für die Zertifikatsverwaltung
Kennwortschutz für den privaten Schlüssel
Der private Schlüssel ist geheim und muss mit einem Kennwort geschützt werden, um die Sicherheit zu garantieren.
Geben Sie ein Kennwort ein, um den zu exportierenden privaten Schlüssel zu verschlüsseln.
Kennwort:
******
Kennwortbestätigung:
******
< Zurück
Weiter >
Abbrechen

Abbildung 93: Geben Sie ein Passwort ein

7) Geben Sie die Datei an, in der ihr privater Schlüssel und das Zertifikat gespeichert werden sollen. Klicken Sie auf *Weiter*.

Abbildung 94: Angabe des Speicherorts

8) Klicken Sie auf *Fertig stellen*.

Abbildung 95: Fertigstellung des Exports

9) Die Dateiendung muss nun noch von „.pfx“ in „.p12“ umbenannt werden. Verwenden Sie hierfür Ihr Datei-Verwaltungsprogramm, wie zum Beispiel den Windows-Explorer.

Die exportierte PKCS#12-Datei (*.p12) können Sie nun für Ihre Client-Anwendung verwenden.

5.6 Hinweise zum Einsatz des Internet Explorers

Wenn Sie als Browser den Internet Explorer einsetzen, dann müssen Sie vor der ersten Benutzung Ihr Zertifikat, welches sich auf der Smartcard befindet, dem Browser bekannt machen. Wenn Sie selbst das Zertifikat mit diesem Browser beantragt bzw. erneuert haben, dann ist dies nicht mehr nötig.

Um Ihr Zertifikat dem Browser bekannt zu machen, steht Ihnen ein spezielles Tool zur Verfügung, welches mit der Treiber-Software für den Smartcard-Leser auf Ihrem Arbeitsplatzrechner installiert wurde. Gehen Sie bitte wie folgt vor:

1) Stecken Sie Ihre Smartcard in den Smartcard-Leser ein.
2) Rufen Sie im Windows-Startmenü unter *Programme -> KOBIL Systems -> KOBIL Smart Key* die Funktion *Registrierung der Zertifikate* auf..

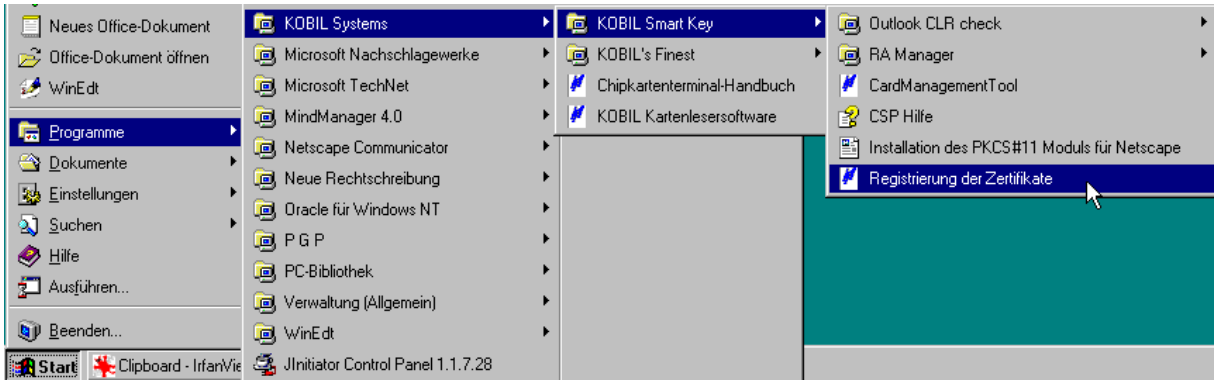

Abbildung 96: Aufruf der Funktion *Registrierung der Zertifikate*

3) Es erscheint der Import-Assistent für die Zertifikatsverwaltung. Klicken Sie *Weiter*.

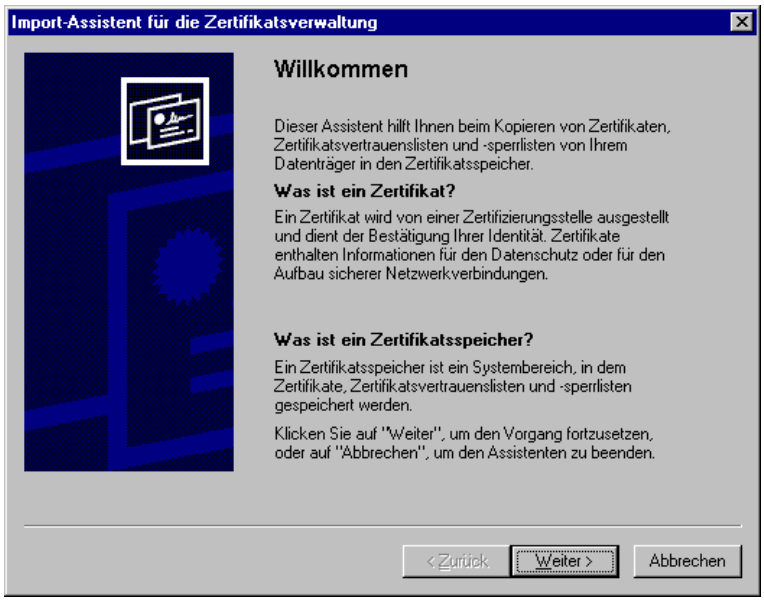
Import-Assistent für die Zertifikatsverwaltung
Willkommen
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatsvertrauenslisten und -sperrlisten von Ihrem Datenträger in den Zertifikatsspeicher.
Was ist ein Zertifikat?
Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und dient der Bestätigung Ihrer Identität. Zertifikate enthalten Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen.
Was ist ein Zertifikatsspeicher?
Ein Zertifikatsspeicher ist ein Systembereich, in dem Zertifikate, Zertifikatsvertrauenslisten und -sperrlisten gespeichert werden.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen, oder auf "Abbrechen", um den Assistenten zu beenden.
< Zurück
Weiter >
Abbrechen

Abbildung 97: Import-Assistent

4) Der Import-Assistent fordert Sie auf, den Zertifikatsspeicher anzugeben. Verwenden Sie die angegebene Option und Klicken Sie *Weiter*.

Import-Assistent für die Zertifikatsverwaltung
Zertifikatsspeicher auswählen
Zertifikatsspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Wählen Sie den Zertifikatsspeicher für die neuen Zertifikate.
Zertifikatsspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatsspeicher:
Durchsuchen...
< Zurück
Weiter >
Abbrechen

Abbildung 98: Auswahl des Zertifikatsspeichers

5) Beenden Sie den Import-Assistenten durch Klicken des Button *Fertig stellen*.

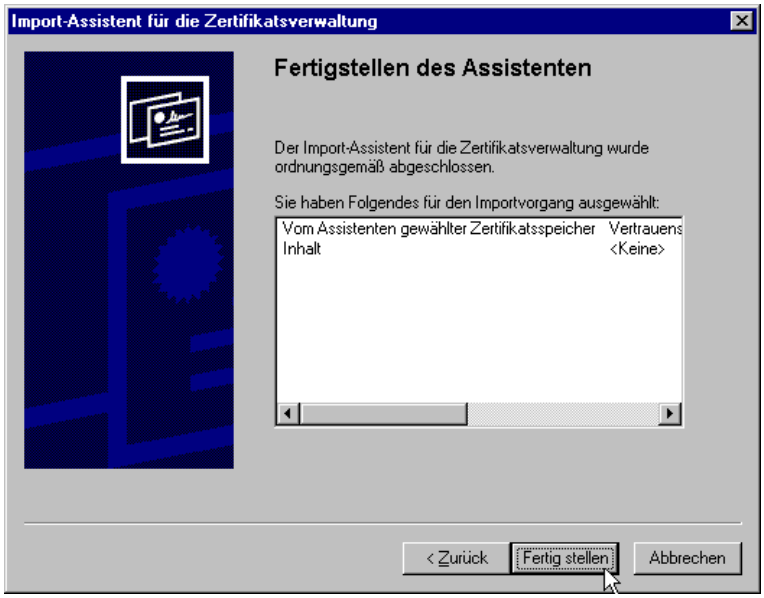

Abbildung 99: Fertigstellung des Import-Assistenten

6) Sie erhalten eine entsprechende Meldung. Klicken Sie *OK*.

Abbildung 100: Weiter mit *OK*

7) Es folgt eine Abfrage, ob die Zertifikate der Smartcard nun registriert werden sollen. Klicken Sie *Ja*.

Zertifikate registrieren
Wollen Sie, daß Smart Key die Zertifikate auf Ihrer Chipkarte automatisch registriert?
Ja
Nein

Abbildung 101: Klicken Sie *Ja* zum Import Ihres Zertifikats

8) Geben Sie nun die PIN Ihrer Smartcard am Smartcard-Terminal ein und drücken Sie an der Tastatur des Terminals die Bestätigungstaste.

Abbildung 102: Sie müssen Ihre PIN an der Tastatur des Smartcard-Terminals eingeben

9) Ihr Zertifikat wird von der Smartcard gelesen und in den Browser importiert.

Abbildung 103: Automatisches Auslesen des Zertifikats

10) Auf Ihrer Smartcard befinden sich mehrere Speicherbereiche für Zertifikate. Das verwendete Tool versucht nun, aus allen Speicherplätzen die Zertifikate herauszulesen. Da Ihre Smartcard aber nur

ein Zertifikat (bei Single Key) bzw. zwei Zertifikate (bei Dual Key) enthält, erscheint beim Versuch, die anderen Speicherplätze auszulesen eine Fehlermeldung[3]. Klicken Sie auf *Abbrechen*.

Abbildung 104: Fehlermeldung beim Versuch, weitere Zertifikate von der Smartcard zu lesen

Ihr Zertifikat ist nun in der Browser-Datenbank gespeichert. Der private Schlüssel befindet sich jedoch ausschließlich auf der Smartcard. Sie können daher das im Browser eingetragene Zertifikat nur in Verbindung mit Ihrer Smartcard verwenden.

Wenn auf Ihrem Arbeitsplatzrechner eine neue Version des Internet Explorers installiert wird, dann wird unter Umständen auch eine neue Browser-Datenbank angelegt. In dieser ist Ihr Zertifikat nicht gespeichert. Daher müssen Sie bei einem Browserwechsel oder bei Verwendung eines neuen Systems Ihr Zertifikat erst wieder dem Browser bekannt machen.

[3] Wenn Sie auf Ihrer Smartcard Zertifikate für weitere Anwendungen gespeichert haben, werden diese ausgelesen und in Ihrem Browser gespeichert. Wenn Sie dies nicht wünschen, können Sie die Zertifikate manuell aus Ihrem Browser löschen (Menü *Extras* > *Internetoptionen* > *Inhalt* > *Zertifikate* > *Eigene Zertifikate*)

6 SICHERHEITSHINWEISE

Voraussetzung für die Sicherheit von T-TeleSec MailPass ist, dass Sie mit dem Ihnen zur Verfügung gestellten PSE und allen in Zusammenhang mit T-TeleSec MailPass stehenden Informationen (zum Beispiel PIN, Sperrpasswort) sachgerecht umgehen. Aus diesem Grund sollten Sie auf jeden Fall die im Folgenden aufgeführten Sicherheitshinweise beachten.

6.1 Ihre Smartcard

Falls Sie zur Speicherung Ihres privaten Schlüssels eine Smartcard verwenden, dann ist dieser in der gegenwärtig bestmöglichen Form geschützt. Ein Auslesen des privaten Schlüssels ist nahezu unmöglich. Gleiches gilt für eine Verwendung der Smartcard ohne PIN-Eingabe oder das Kopieren der Smartcard. Das Erraten einer PIN durch bloßes Durchprobieren ist ebenfalls so gut wie ausgeschlossen, da sich die Karte nach drei hintereinander eingegebenen falschen PINs selbst sperrt. Trotz dieser Sicherheitsvorkehrungen kann natürlich auch eine Smartcard keine perfekte Sicherheit bieten und muss daher geschützt werden. Grundsätzlich sind dabei zwei Belange zu beachten: Zum einen darf niemand Zugang zu ihrer Smartcard erhalten und zum anderen darf niemand ihre PIN erfahren. Ein Missbrauch ist zwar nur möglich, wenn ein Angreifer auf Smartcard und PIN gleichzeitig zugreifen kann. Um eine größtmögliche Sicherheit zu erreichen, sollten Sie jedoch sowohl den Zugang zur Smartcard als auch zur PIN schützen.

Für den Schutz der Smartcard gelten folgende Richtlinien:

- Halten Sie Ihre Smartcard unter Verschluss und schützen Sie sie vor Diebstahl!
- Entfernen Sie Ihre Smartcard aus dem Leser, wenn Sie sie nicht mehr verwenden!
- Geben Sie Ihre Smartcard nicht an andere weiter, auch nicht leihweise!
- Lassen Sie nach Verlust Ihrer Smartcard das Zertifikat (bzw. die Zertifikate) unverzüglich sperren!

Die PIN, mit der Ihre Smartcard geschützt ist, ist eine sechsstellige Geheimzahl, die Sie selbst wählen und verändern können. Beachten Sie bitte folgende Richtlinien für den Schutz der PIN:

- Wählen Sie keine leicht zu erratende Zahl, wie zum Beispiel Ihr Geburtsdatum oder sechsmal dieselbe Ziffer!
- Wählen Sie nach Möglichkeit keine Zahl, die Sie auch an anderer Stelle als Geheimzahl oder PIN verwenden!
- Ändern Sie Ihre PIN nach Möglichkeit mindestens einmal jährlich!
- Achten Sie darauf, dass niemand Ihre PIN bei der Eingabe erspähen kann!
- Teilen Sie Ihre PIN auf keinen Fall einem Anderen mit! Auch Mitarbeiter der T-TeleSec werden Sie nie nach Ihrer PIN fragen.
- Notieren Sie Ihre PIN nach Möglichkeit nicht, sondern merken Sie sich Ihre PIN!
- Falls Sie sich Ihre PIN doch notieren, bewahren Sie die Notiz unbedingt getrennt von Ihrer Smartcard auf und achten Sie darauf, dass niemand Zugang dazu hat!

6.2 Ihr Software-PSE

Falls Sie keine Smartcard als Speicher für den privaten Schlüssel einsetzen, wird dieser in einem so genannten Software-PSE gespeichert. Dabei handelt es sich um eine verschlüsselte Datei (.p12 oder .pfx), die mit einem Passwort geschützt ist. Im Vergleich zu einer Smartcard bietet ein Software-PSE eine geringere Sicherheit. Es ist daher noch mehr als bei einer Smartcard notwendig, dass Sie Ihr Software-PSE durch geeignete Maßnahmen schützen. Grundsätzlich sind dabei zwei Belange zu

beachten: Zum einen darf niemand Zugang zu ihrem PSE haben und zum anderen darf niemand Ihr Passwort erfahren. Ein Missbrauch ist zwar nur möglich, wenn ein Angreifer PSE und Passwort besitzt. Um eine größtmögliche Sicherheit zu erreichen, sollten Sie jedoch sowohl den Zugang zum PSE als auch das Passwort schützen.

Um keinem Angreifer Zugang zum Software-PSE zu ermöglichen, beachten Sie bitte folgende Richtlinien. Da eine Datei im Gegensatz zu einer Smartcard einfach kopiert werden kann, sind diese Hinweise besonders wichtig:

- Erzeugen Sie nur eine Sicherheitskopie der Datei und verwahren Sie diese an einem sicheren Ort!
- Speichern Sie die Datei ausschließlich auf einer Diskette oder in einem lokalen Verzeichnis!
- Achten Sie darauf, dass niemand Zugriff auf die Datei hat!
- Achten Sie darauf, dass niemand die Datei kopieren kann!
- Geben Sie die Datei nicht an andere weiter, auch nicht vorübergehend!
- Lassen Sie bei Verdacht auf unbefugten Zugang zu Ihrem PSE das Zertifikat (bzw. die Zertifikate) unverzüglich sperren!

Um zu verhindern, dass ein Angreifer Kenntnis ihres Passworts erlangt, sind weitere Maßnahmen notwendig. Im Gegensatz zur Smartcard, die nach der Eingabe dreier falscher PINs ihren Betrieb einstellt, gibt es bei einem Software-PSE keinen Schutz vor dem Durchprobieren beliebig vieler Passwörter. Dies gilt natürlich insbesondere dann, wenn ein Angreifer ungestört mit einer Kopie Ihres Software-PSEs arbeiten kann. Das Durchprobieren von Passwörtern lässt sich sogar automatisieren, wodurch ein Angreifer mehrere Tausend Passwörter pro Sekunde testen kann. Es ist keine Seltenheit, dass Hacker diese Möglichkeit nutzen, um ganze Wörterbücher durchzuprobieren und dabei auch hunderte abgewandelter Schreibweisen (beispielsweise „telefon“, „tELEFON“, „Telef0n“, ...) einbeziehen. Beachten Sie daher die aufgeführten Richtlinien für die Wahl Ihres Passworts. Diese sollten Sie außerdem beachten, wenn Sie Ihr Zertifikat selbst mit Ihrem Browser beantragt haben oder wenn Sie Ihr Zertifikat erneuern. In diesem Fall befindet sich Ihr privater Schlüssel in der Datenbank Ihres Web-Browsers, die ebenfalls mit einem Passwort geschützt ist. Auf dieses Passwort sollten Sie die gleichen Sicherheitsvorkehrungen anwenden. Im Einzelnen gelten folgende Richtlinien:

- Wählen Sie kein Passwort, das ein sinnvolles Wort darstellt (beispielsweise „Hund“, „Unterhaching“ oder „Telekom“)! Viele Hacker verwenden Wortdateien, in denen auch ungebräuchliche, fremdsprachige, geografische und fachspezifische Begriffe enthalten sind. Insbesondere sollten Sie auch keinen Begriff aus ihrer unmittelbaren Umgebung (Name, Wohnort, ...) wählen.
- Wählen Sie kein Passwort, das aus einem sinnvollen Wort abgeleitet ist (beispielsweise „hUNd“ oder „Dnuh“)! Es gibt spezielle Computerprogramme, die aus einem Wort hunderte anderer Wörter ableiten und dabei alle denkbaren Verwürfelungen und Ersetzungen einbeziehen.
- Verwenden Sie Passwörter, die mindestens acht Zeichen lang sind!
- Ein Passwort sollte sowohl Groß- und Kleinbuchstaben als auch Ziffern und Sonderzeichen enthalten!
- Auch für Hacker schwer zu erraten gelten beispielsweise Passwörter, die aus zwei voneinander unabhängigen Wörtern bestehen, die durch ein zusätzliches Zeichen getrennt sind. Beispiele dafür sind etwa „hype%Sonne“ oder „unna-Steckdose“. Ähnlich sicher sind Kunstwörter, die sich aus den Anfangsbuchstaben eines Satzes ergeben, also etwa „MH,dh4E“ (*M*ein *H*ut, *d*er *h*at *4 E*cken).
- Achten Sie darauf, dass niemand Ihr Passwort bei der Eingabe erspähen kann!
- Ändern Sie Ihr Passwort nach Möglichkeit mindestens einmal jährlich!
- Teilen Sie Ihr Passwort auf keinen Fall einem Anderen mit!
- Notieren Sie Ihr Passwort nach Möglichkeit nicht, sondern merken Sie sich Ihr Passwort!

- Falls Sie sich Ihr Passwort doch notieren, bewahren Sie die Notiz unbedingt getrennt von dem Computer (bzw. der Diskette) auf, welcher Ihr Software-PSE enthält, und achten Sie darauf, dass niemand Zugang zu dem notierten Passwort hat!

6.3 Weitere Richtlinien

Bitte beachten Sie zusätzlich folgende weitere Richtlinien:

- Bewahren Sie die Telefonnummer oder die E-Mail-Adresse für die Sperrung so auf, dass Sie sie im Bedarfsfall greifbar haben.
- Ihr MailPass-Zertifikat ist **ausschließlich** für die Verschlüsselung und Signatur von E-Mails und Dateien sowie zur Authentifizierung gegenüber Web-Servern bestimmt. Für weitere Anwendungen stellt Ihnen das Telekom Trust Center die dafür geeigneten Zertifikate zur Verfügung. Für nähere Informationen wenden Sie sich bitte an Ihren MailPass-Verantwortlichen.
- Das Ihnen ausgehändigte Passwort für Sperrungen darf nicht an andere weitergegeben werden.
- Das Ihnen ausgehändigte Passwort für den Zugang zur Benutzer-Web-Schnittstelle und zur eingeschränkten Benutzer-Web-Schnittstelle darf nicht an andere weitergegeben werden.

7 PROBLEME UND LÖSUNGEN

Sie haben über die Benutzer-Web-Schnittstelle ein Zertifikat beantragt und warten vergeblich auf die Meldung zur Abholung des Zertifikats.

Es gibt zwei mögliche Ursachen: Entweder ist die von Ihnen im Zertifikatsantrag angegebene E-Mail-Adresse nicht korrekt oder Ihr Sub-Registrator hat Ihren Zertifikatsantrag noch nicht bearbeitet.
Wenden Sie sich in beiden Fällen bitte an Ihren Sub-Registrator.

Bei der Erneuerung Ihres Zertifikats über die (eingeschränkte) Benutzer-Web-Schnittstelle wird vom Browser Ihr Zertifikat nicht zur Auswahl angeboten.

Beim Einsatz von Smartcards:

Prüfen Sie, ob der Smartcard-Leser korrekt angeschlossen ist. Prüfen Sie, ob Ihre Smartcard richtig im Smartcard-Leser eingesteckt ist.

Möglicherweise wird die Smartcard von einer anderen Anwendung blockiert.

Bei Verwendung des Internet Explorer muss Ihr Zertifikat vor erstmaliger Verwendung dem Browser bekannt gemacht werden. Befolgen Sie hierfür die Hinweise in Kapitel 5.6.

Beim Einsatz von Software-PSEs:

Ihr Zertifikat und der private Schlüssel müssen zur Erneuerung in den Browser importiert werden. Befolgen Sie hierfür die Hinweise in Kapitel 5.3.2.

Bei der Erneuerung wird Ihr Zertifikat nicht akzeptiert.

Prüfen Sie zunächst, ob Sie das richtige Zertifikat ausgewählt haben. Wenn dies der Fall ist, ist das Zertifikat entweder abgelaufen oder gesperrt. Wenden Sie sich an Ihren Sub-Registrator, um ein neues Zertifikat zu erhalten.

Hinweis: Um sicherzustellen, dass der Grund der Zurückweisung die Ungültigkeit Ihres Zertifikats ist, sollten Sie zunächst die Gültigkeit des Zertifikats überprüfen. Eine entsprechende Anfrage können Sie mit der Funktion *Zertifikat prüfen* über die (eingeschränkte) Benutzer-Web-Schnittstelle ausführen. Hierfür müssen Sie die Seriennummer Ihres Zertifikats angeben.

Ihr Zertifikat ist ungültig.

Entweder ist die Gültigkeitsdauer des Zertifikats abgelaufen, ohne das es erneuert wurde, oder das Zertifikat wurde gesperrt. Sollten Sie nicht über die Sperrung des Zertifikats informiert sein, klären Sie dies umgehend mit Ihrem Sub-Registrator.
Der Sub-Registrator kann Ihnen ein neues Zertifikat ausstellen, bzw. einen von Ihnen neu gestellten Zertifikatsantrag bearbeiten.

Sie müssen das Zertifikat sperren lassen und wissen das Sperrpasswort nicht mehr.

Wenden Sie sich an Ihren Sub-Registrator. Dieser kann Ihr Zertifikat auch ohne Angabe des Sperrpassworts sperren lassen. Allerdings müssen Sie sich gegenüber dem Sub-Registrator authentisieren, zum Beispiel durch persönliches Erscheinen.

Sie sind mit Ihren Browser an einer anderen Web-Schnittstelle (Master-RA, Sub-RA oder anderer Web-Server, zum Beispiel für Online-Banking) über ein Zertifikat oder Benutzername / Passwort angemeldet und wollen sich nun an der (eingeschränkten) Benutzer-Web-Schnittstelle anmelden.

Dies erfordert das Beenden und den Neustart des Browsers. Anschließend können Sie die URL der (eingeschränkten) Benutzer-Web-Schnittstelle aufrufen und sich mit Benutzername und Passwort anmelden.

Bei Problemen, welche nicht in dieser Übersicht behandelt werden, wenden Sie sich bitte an Ihren MailPass-Verantwortlichen.

GLOSSAR

Additional Decryption Key	Zusätzliches Schlüsselpaar zur Ver- und Entschlüsselung von Daten, für den Fall, dass der private Benutzerschlüssel nicht zugänglich ist.
ADK	Siehe Additional Decryption Key.
ARL	Siehe Authority Revocation List.
Authority Revocation List	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsinstanzen aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsinstanz sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
Benutzer	Person, die ein MailPass-Zertifikat und den dazu gehörenden privaten Schlüssel verwendet.
Benutzer-Web-Schnittstelle	Web-basierte Komponente, über die Benutzer ihr Zertifikat verwalten können (Beantragung, Erneuerung, Sperrung etc.).
Betreiber-Domain	Bereich, in dem ein T-TeleSec-Kunde (Domain-Betreiber) MailPass-Zertifikate einsetzt. Die Betreiber-Domain ist durch einen festzulegenden Namen gekennzeichnet, der in den Zertifikaten aufgeführt ist.
CA	Certification Authority. Siehe Zertifizierungsinstanz.
Certificate Policy	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Revocation List	Siehe Sperrliste.
Certification Authority	Siehe Zertifizierungsinstanz.
Certification Practice Statement	Richtlinien für den Betrieb einer Zertifizierungsinstanz. Insbesondere umfasst das CPS alle CPs einer Zertifizierungsinstanz.
Chipkarte	Plastikkarte mit integriertem Computerchip. Telefonkarten sind ein Beispiel dafür. Ist der Computerchip dazu in der Lage, Berechnungen durchzuführen, so spricht man auch von einer Smartcard. Smartcards können auch für kryptografische Anwendungen eingesetzt werden.
CP	Siehe Certificate Policy.
CPS	Siehe Certification Practice Statement.
CRL	Certificate Revocation List. Siehe Sperrliste.
Data Recovery	Mechanismus zur Datenwiederherstellung. Diese kann notwendig sein, wenn eine Datei nicht mit dem entsprechenden Benutzerschlüssel entschlüsselt werden kann (etwa wenn ein Mitarbeiter das Unternehmen verlassen hat).
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Digitales Zertifikat	Datensatz, der den Namen einer Person oder eines Systems, deren öffentlichen Schlüssel, gegebenenfalls einige andere Angaben und eine Signatur einer Zertifizierungsinstanz enthält.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
DN	Siehe Distinguished Name.
Domain-Betreiber	Kunde von T-TeleSec, der T-TeleSec MailPass einsetzt. Jedem Domain-Betreiber ist eine Betreiber-Domain zugeordnet.
Dual Key	Variante von T-TeleSec MailPass, bei der für Verschlüsselung und

	Signatur getrennte Schlüsselpaare verwendet werden, das heißt ein Benutzer besitzt zwei entsprechende Zertifikate.
Eingeschränkte Benutzer-Web-Schnittstelle	Web-basierte Komponente, über die Benutzer ihr Zertifikat verwalten können. Gegenüber der vollständigen Benutzer-Web-Schnittstelle ist allerdings keine Beantragung von Zertifikaten möglich, sondern lediglich eine Erneuerung.
Elektronische Signatur	Siehe digitale Signatur.
Hardware Security Modul	Hardwarebox zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hash-Wert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
HSM	Siehe Hardware Security Modul.
Key Recovery	Mechanismus zur Schlüsselwiederherstellung. Diese kann notwendig sein, wenn ein Benutzer seinen Schlüssel (etwa durch eine beschädigte Datei) verliert.
Kompromittierung	Ein geheimer Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
LDAP	Siehe Lightweight Directory Access Protocol.
LDAP-Server	Server, der Informationen speichert, die über LDAP abrufbar sind.
Lightweight Directory Access Protocol	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
MailPass CA	Zertifizierungsinstanz, die im Rahmen von T-TeleSec MailPass zum Einsatz kommt.
Mail-Request	Variante eines Zertifikatsantrags, bei dem die Daten per E-Mail an die Zertifizierungsinstanz übermittelt werden.
Master-Domain	Siehe Betreiber-Domain.
Master-RA	Web-basierte Komponente, die vor allem dem Management von Sub-Registrator-Zertifikaten und der Definition von Zuständigkeitsbereichen dient (wird vom Master-Registrator verwendet).
Master-Registrator	Mitarbeiter des Domain-Betreibers, der für das Management von Sub-Registrator-Zertifikaten verantwortlich ist.
OCSP	Das Online Certificate Status Protocol ermöglicht die Online-Abfrage der Gültigkeit von Zertifikaten.
PIN	Personal Identification Number. Geheimzahl, wie sie zum Beispiel am Geldautomaten verwendet wird.

PKI	Siehe Public-Key-Infrastruktur.
PKIX	Public Key Infrastructure X.509. Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
PKS	Public Key Service. Service von T-TeleSec zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Policy	Richtlinien, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
PSE	Personal Security Environment. In der persönlichen Sicherheitsumgebung sind sicherheitsrelevante Informationen wie der private Schlüssel gespeichert. Das PSE kann als verschlüsselte Datei oder auf einer Smartcard vorliegen und ist durch ein Passwort bzw. eine PIN geschützt.
Public-Key-Infrastruktur	Gesamtheit der Komponenten, Prozesse und Konzepte, die zur Verwendung von Public-Key-Verfahren verwendet werden. Typischerweise besteht eine Public-Key-Infrastruktur aus zentralen Komponenten wie einer Zertifizierungsinstanz und einem Verzeichnisdienst und verschiedenen Client-Komponenten.
RA	Registration Authority. Siehe Registrierungsinstanz.
Registration Authority	Siehe Registrierungsinstanz.
Registrierungsinstanz	Komponente, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten.
Root CA	Siehe Wurzelzertifizierungsinstanz.
RSA	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
S/MIME	Secure Multipurpose Internet Mail Extension. Erweiterung des E-Mail-Formats MIME, die Zusätze für kryptografische Dienste beschreibt, welche Authentizität, Integrität und Vertraulichkeit von Nachrichten sicherstellen.
Schlüssel	Ein Schlüssel bezeichnet in der Kryptografie eine geheime Information (geheimer Schlüssel) oder ein öffentliches Gegenstück dazu (öffentlicher Schlüssel). Es gibt Verfahren, bei denen jeweils mit dem gleichen geheimen Schlüssel ver- und entschlüsselt wird sowie Verfahren bei denen ein öffentlicher Schlüssel zum Ver- und ein geheimer zum Entschlüsseln verwendet wird.
Secure Socket Layer	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet. Kann ihn vielen Fällen statt dem komplexeren IPSec verwendet werden.
Signatur	Siehe digitale Signatur.
Single Key	Variante von T-TeleSec MailPass, bei der für Verschlüsselung und Signatur das selbe Schlüsselpaar verwendet wird, das heißt ein Benutzer besitzt ein Zertifikat.
Smartcard	Chipkarte mit Rechenfunktionalität, die für kryptografische Zwecke verwendet werden kann. Im Rahmen von T-TeleSec MailPass kommt die NetKey Karte zum Einsatz.
Software-PSE	Durch Verschlüsselung geschützte Datei zur Speicherung des privaten Schlüssels eines Benutzers.
Sperr-Hotline	Zentrale Hotline für T-TeleSec MailPass, die ausschließlich für das Sperren von Zertifikaten (Benutzer- und Sub-Registrator-Zertifikate)

	zuständig ist.
Sperr-Hotline-Operator	Mitarbeiter der Sperr-Hotline, der die Sperr-Hotline-Web-Schnittstelle bedient.
Sperr-Hotline-Web-Schnittstelle	Web-basierte Komponente, die ausschließlich dem Sperren von Zertifikaten dient (wird von Sperr-Hotline-Operator genutzt).
Sperrinstanz	Komponente, die Zertifikatssperrungen durchführt.
Sperrliste	Liste, in der gesperrte digitale Zertifikate aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats sollte anhand einer Sperrliste überprüft werden, ob dieses noch verwendet werden darf. Wird auch als Certificate Revocation List (CRL) bezeichnet.
SSL	Siehe Secure Socket Layer.
Sub-Domain	Siehe Zuständigkeitsbereich.
Sub-RA	Web-basierte Komponente zur Verwaltung von Benutzerzertifikaten (wird vom Sub-Registrator bedient).
Sub-Registrator	Mitarbeiter des MailPass-Domain-Betreibers, der für das Management von Benutzerzertifikaten verantwortlich ist.
Telekom Trust Center	Speziell geschütztes Gebäude, in dem unter besonderen Sicherheitsvorkehrungen Zertifizierungsinstanzen und weitere PKI-Komponenten betrieben werden.
TTC	Siehe Telekom Trust Center.
TTC-Operator	Mitarbeiter von T-TeleSec, der insbesondere für die Registrierung von Master-Registratoren zuständig ist.
TTC-RA	Web-basierte Komponente zum Management von Master-Registratoren (wird vom TTC-Operator bedient).
Verantwortlicher des Domain-Betreibers	Mitarbeiter des Domain-Betreibers, der als Ansprechpartner und Gesamtverantwortlicher fungiert.
Verzeichnisdienst	Datenspeicher, der den Abruf von Zertifikaten und Informationen über Zertifikate (insbesondere Sperrlisten) ermöglicht.
Web-Request	Variante eines Zertifikatsantrags, bei dem die Daten über ein Web-Formular an die Zertifizierungsinstanz übermittelt werden.
Wurzelzertifizierungs-instanz	Oberste Zertifizierungsinstanz einer CA-Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsinstanz ausgestellt wurde, sondern selbstsigniert ist.
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zertifikat	Siehe digitales Zertifikat.
Zertifizierungsinstanz	Komponente, die digitale Zertifikate ausstellt, indem sie einen Datensatz bestehend aus öffentlichem Schlüssel, Name und verschiedenen anderen Daten digital signiert. Ebenso werden von der Zertifizierungsinstanz Sperrinformationen herausgegeben.
Zuständigkeitsbereich	Teilbereich einer Betreiber-Domain.